Exhibit 11

KuCoin Hack

Saturday, July 13, 2024 10:08 PM

On September 25, 2020, KuCoin announced on their website that they were hacked:

The next day, they posted an update with additional details:

kucoin.com/announcement/en-kucoin-ceo-livestream-recap-l...

KUCOIN Buy Crypto Markets Trade Derivatives Earn Institutional More

Home / Announcements / KuCoin CEO Livestream Recap - Latest Updates About Security Incident

KuCoin CEO Livestream Recap - Latest Updates About Security Incident

09/26/2020, 03:56:54

In response to the recent KuCoin Security Incident, KuCoin Global CEO Johnny Lyu hosted a livestream at 12:30 (UTC+8) on September 26, 2020, and announced more updates regarding the incident.

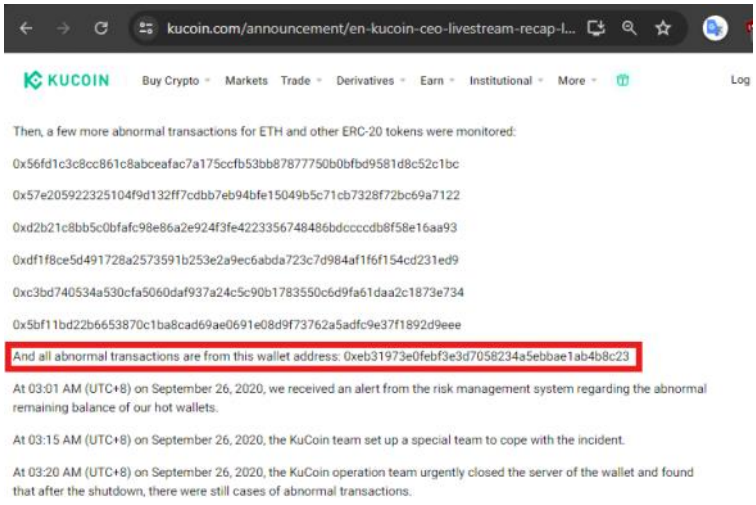
He mentioned that, according to the latest internal security audit report, part of the Bitcoin, ERC-20 and other tokens in KuCoin's hot wallets were transferred out of the exchange, which contained few parts of the total assets holdings. The assets in the cold wallets are safe and unharmed, and the hot wallets have been re-deployed.

We are locating the reason for the incident, and will keep users updated once it is confirmed. **Please rest assured that if any user fund is affected by this incident, it will be covered completely by KuCoin and our insurance fund.**

Here's the recap of the livestream.

Johnny first explained the timeline of the incident as below:

In this announcement, KuCoin stated that the hacker's wallet address was 0xeb31...8c23:



kucoin.com/announcement/en-kucoin-ceo-livestream-recap-l...

KUCOIN Buy Crypto Markets Trade Derivatives Earn Institutional More Log

Then, a few more abnormal transactions for ETH and other ERC-20 tokens were monitored:

0x56fd1c3c8cc861c8abceafac7a175ccfb53bb87877750b0bfbd9581d8c52c1bc

0x57e205922325104f9d132ff7cdbb7eb94bfe15049b5c71cb7328f72bc69a7122

0xd2b21c8bb5c0bfafc98e86a2e924f3fe4223356748486bdcccdb8f58e16aa93

0xdf1f8ce5d491728a2573591b253e2a9ec6abda723c7d984af1f6f154cd231ed9

0xc3bd740534a530cfa5060daf937a24c5c90b1783550c6d9fa61daa2c1873e734

0x5bf11bd22b6653870c1ba8cad69ae0691e08d9f73762a5adfc9e37f1892d9eee

And all abnormal transactions are from this wallet address: 0xeb31973e0febf3e3d7058234a5ebbae1ab4b8c23

At 03:01 AM (UTC+8) on September 26, 2020, we received an alert from the risk management system regarding the abnormal remaining balance of our hot wallets.

At 03:15 AM (UTC+8) on September 26, 2020, the KuCoin team set up a special team to cope with the incident.

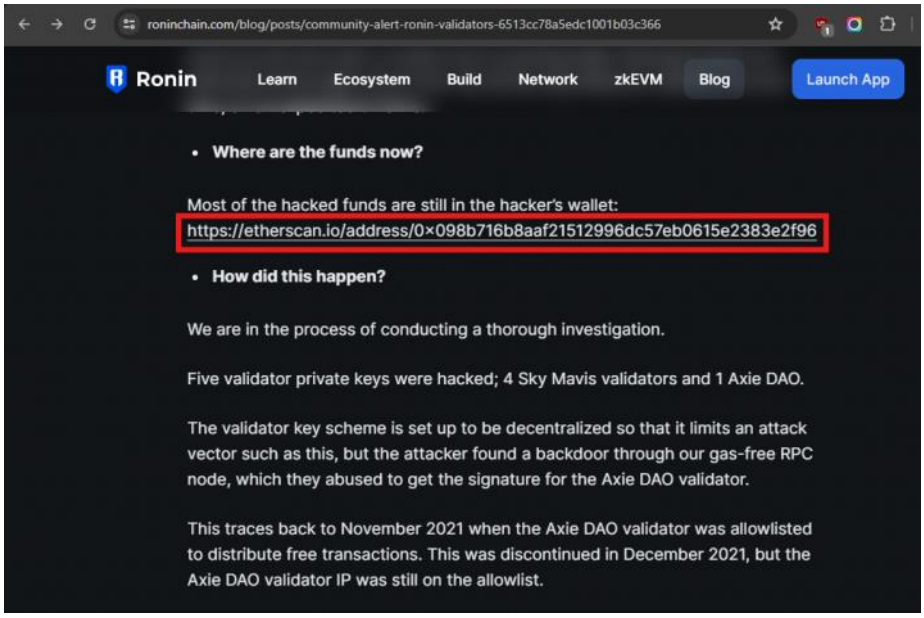
At 03:20 AM (UTC+8) on September 26, 2020, the KuCoin operation team urgently closed the server of the wallet and found that after the shutdown, there were still cases of abnormal transactions.

Using Etherscan, I can see the four transactions that where the KuCoin hacker transferred approximately 11,486 ETH ($4.04 mm) :

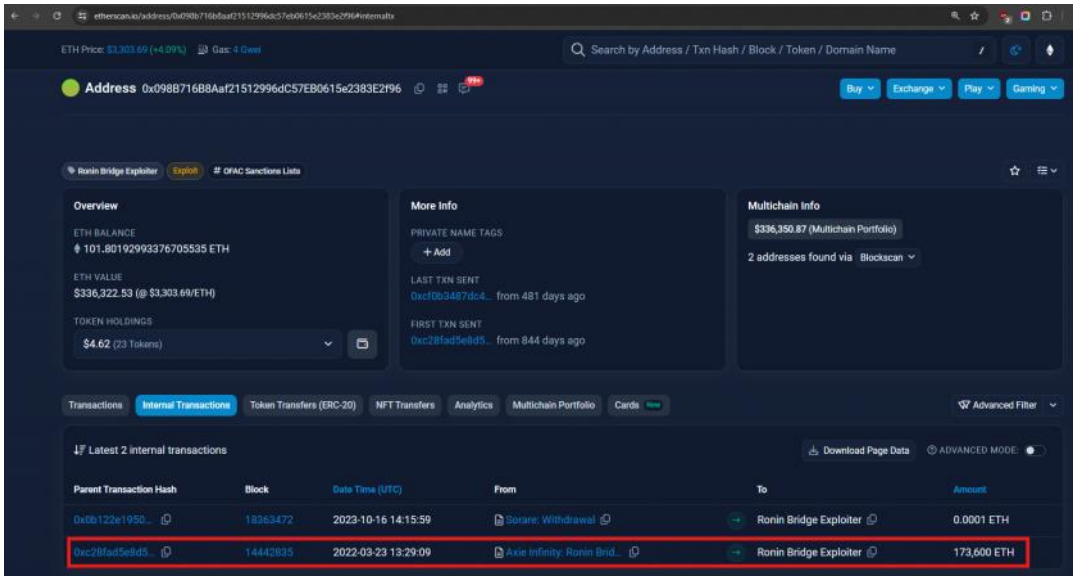
Axie Infinity

Sunday, July 14, 2024 10:22 PM

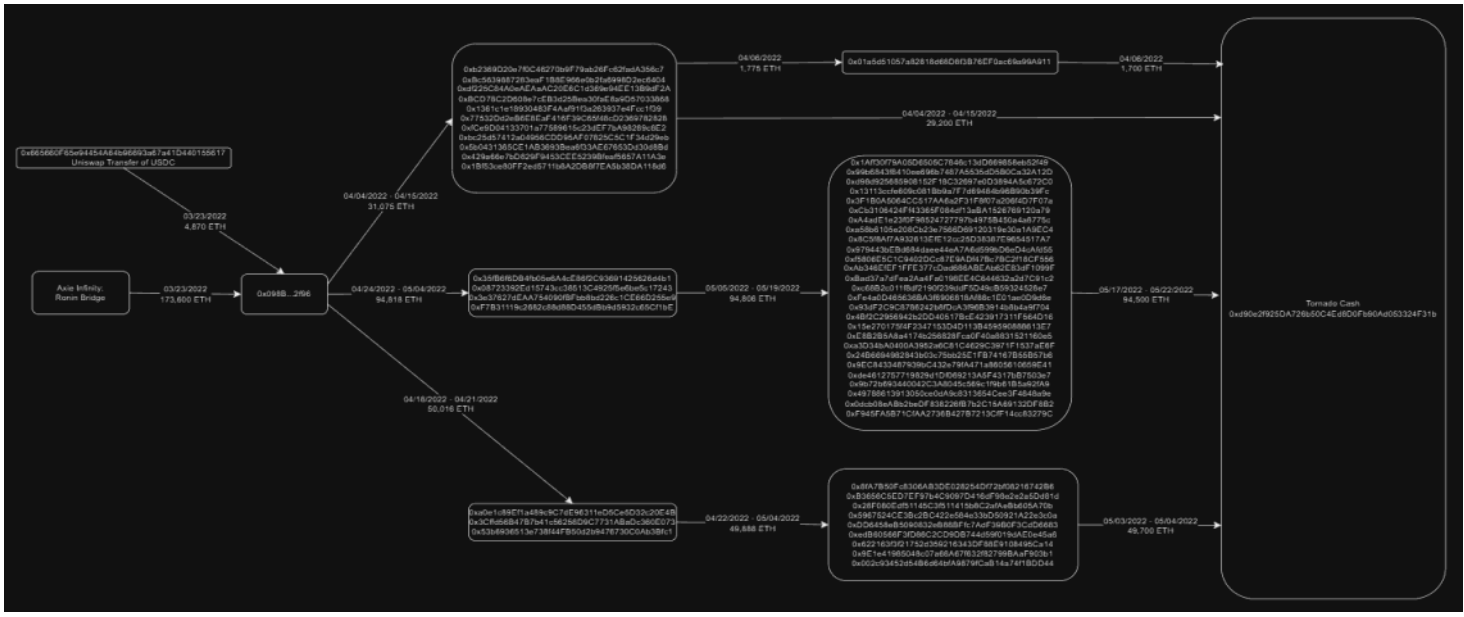
On March 29, 2022, Ronin announced on their blog roninchain.com/blog that Ronin bridge had been hacked for 173,600 ETH and 25,500,000 USDC. The blog post details the two malicious transaction and it reveals the destination wallet of the stolen funds: 0x098b716b8aaf21512996dc57eb0615e2383e2f96



Here is the transaction showing the 173,600 ETH moving to the hacker's wallet on 03/23/2022:



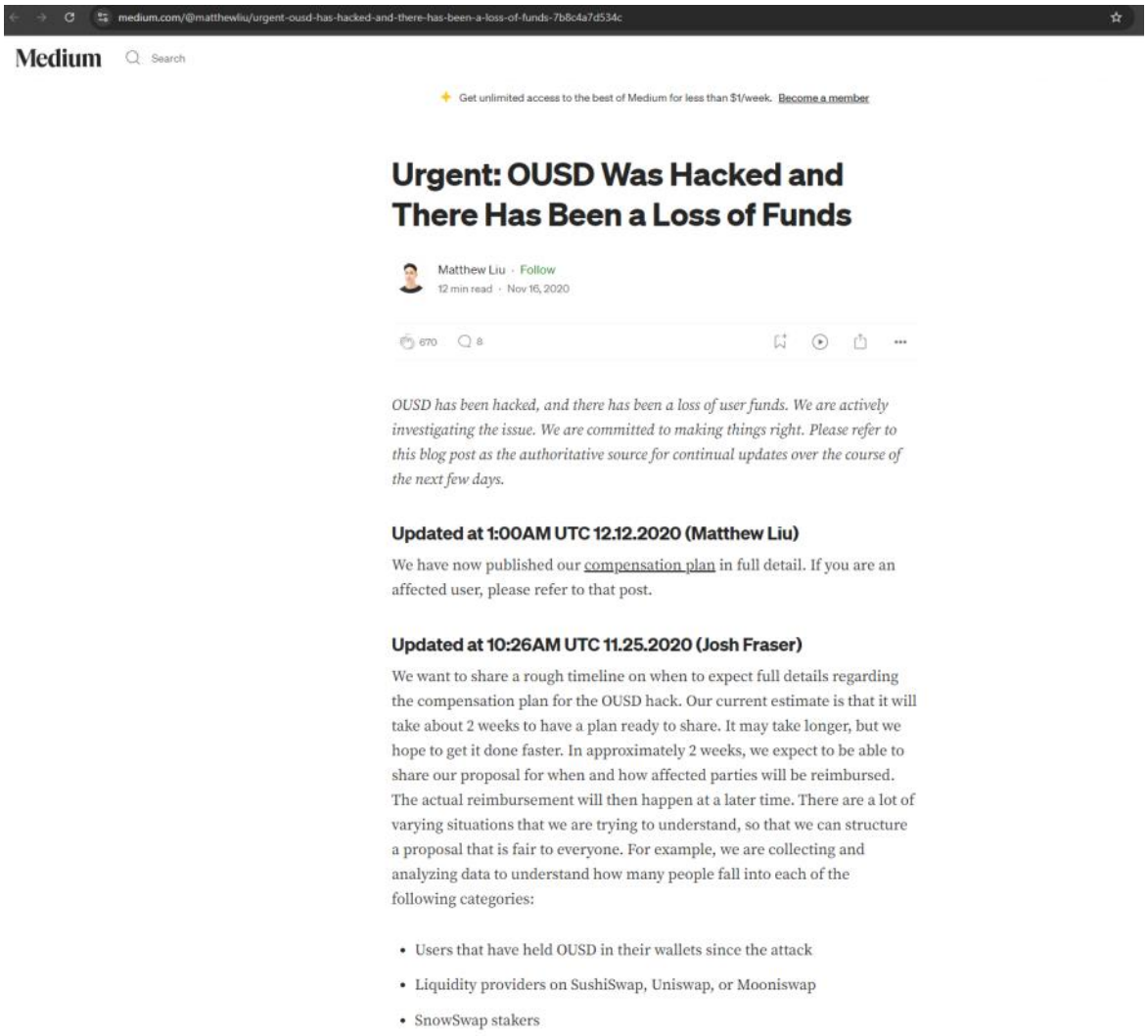
The stolen 173,600 ETH was combined with 4,870 ETH that was swapped for Tether. The ETH was moved through a series of intermediary wallets between 04/04/2022 and 05/19/2022. Between 04/04/2022 and 05/22/2022, 175,100 ETH was transferred to Tornado Cash. The total amount transferred to Tornado Cash was approximately $449.0 million.


0x66566CF65e94454A64b96893a67a41D440155617
Uniswap Transfer of USDC
03/23/2022
4,870 ETH
Axie Infinity: Ronin Bridge
03/23/2022
173,600 ETH
0x098B...2f96
04/04/2022 - 04/15/2022
31,075 ETH
04/24/2022 - 05/04/2022
94,818 ETH
04/18/2022 - 04/21/2022
50,016 ETH
0xb2369D20e7f0C46270b9F79ab26FC62faaA356c7
0x8c5639887283eaF1B8E966e0b2fa699B02ec6404
0xdf225C84A0eAEAaAC20DEAC1a369e94EC138bdF2A
0x8CD78C2D608e7cE3b325Bea30fsE6a9D57033868
0x1361c1e18930483F4Aaf91f3a283937e4Fcc1f39
0x77532Da2e86EBEaF416F39C6f49bCD3659782428
0x6Ce5D0413701a7758961Sc23dEF7bA9828bdE2
0xbc25d57412a04958CDD95AF07625C5C1F3d29eb
0x5b0431365CE1AB36938ea6G3AE67653d39d8Bd
0x429a6fe7bD629F9453CEE5236ffeaf5657A11A3e
0x1Bf53ce80FF2ed5711b8A2DB8f7EA5b38DA11fa6
04/06/2022
1,775 ETH
0x91a5d51057a82818d68D6f3B76EF0ac69a99A911
04/06/2022
1,700 ETH
04/04/2022 - 04/15/2022
29,200 ETH
0x35fB6f6DB4fb05e6A4cE86f2C93691425626d6b1
0x08723392Ed15743ec38513C4925f5ed6be5c17243
0x3e37627dEAA754090fBFbb8a226c1CE66D255e9
0xF7B3111fc2682c88d88D455d8b9d5932c65Cf1bE
05/05/2022 - 05/19/2022
94,806 ETH
0x1Aff3079A06D6505C7646c13dD669858eb52f49
0x996543B410eed98b7457A553fcd58b0Ca32A12D
0xd96d925685908152F18C32697e0D3894A5c672C0
0x1313ccfe609c681Bb9a7F7d6846b96B90b39Fc
0x3F1B0A506ACC617AA6aF31F9f07a3066D7F07a
0xCb3106424FH3365F084df13aBA152676912Da79
0xA4adE1e23f0F9852427279fb4975B450a4a875fc
0xd5Bd105e208Cb23e786fD6912039e30a1A9ECd
0x8C5f8A7A932613CfE12cc28D38387C9654517A7
0x979443bEBd684daee44eA7A6d599b06eD4cAfd55
0xf586E5C1C94022Dcd87E9AD9d7Bc7BC2f18CF566
0xAb346ECF1FFE377c2ad688ABEAb62CB3dF1099F
0xBad37a7dFea2Aa4Fa0198EE4C644632a2d7C91c2
0xc66b2c011Bdf2190239ddf5D49cB59324526e7
0xFe4aD4656368AbF8f96681bAf88c1E01aeC04e8e
0x93dF2C9C87862421dfDcA3f9BB914b8b4a9f704
0x4B02C2956942b2DD40517BcE423917311F564D16
0x15e27017f36ff23471532f4D113b45959088613E7
0xE6B2b5A8a4174b256828fca0F40a8831521160e5
0xa3D34bA0400A3962e0C81C4629C3971F1537aE6F
0x24B6694982843b03c79ab25E1FB74167B65Bb7e6
0x9EC8433487939bC432e79fA471a860561066fE41
0xde461275779829d1DfD69213A5F4317bB7503e7
0x9b72ef934A004D2CAB545e569c199b81Ba92fA9
0x4978661391305Occ0dA9c8313654Cee3F484de9e
0x0dcb08eABb2beDF838226fB7b2C15A69132DF8B2
0xF945FA5B71cfAA2736B427B7213CfF14cc83279C
0x8fA7B50Fc8306AB3DE028254Df72bf0821674286
0xB3656C5ED7EF97b4C9097D416df79be2e2a5Dd81d
0x28F68cEeffb1145C3f511418dBC2afAeBd65A76b
0x5967524CE3Bc2BC422e584e33bD50921A22e3c0a
0xDD6458e85090832e8688Ffc7AdF39B0F3CdD6683
0xedB6056EF3D66C2CD5DB744d59f019dAE0e45a6
0x622163f3f21752d3592163430F88E9108495Ca14
0x9E1e41985049c07e66A67f632f82799BAaF903b1
0x602c63452d5486d4bfA6879Ca814a74f18DD4d
04/22/2022 - 05/04/2022
49,888 ETH
05/17/2022 - 05/22/2022
94,500 ETH
05/03/2022 - 05/04/2022
49,700 ETH
Tornado Cash
0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b

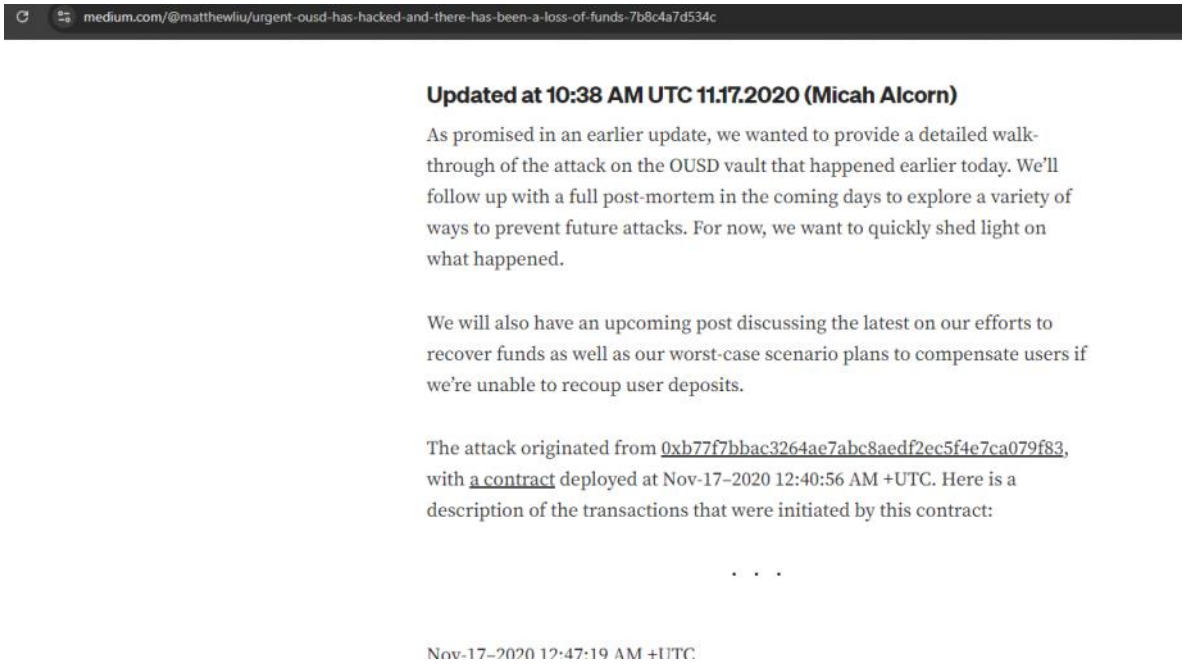
Origin Protocol

Tuesday, September 10, 2024 6:44 PM

On 11/17/2020, Mathew Liu the cofounder of Origin Protocol announced on Origin's blog at medium.com/@matthewliu/ that the Origin Dollar had been hacked and that value was stolen by Ethereum address 0xb77f7bbac3264ae7abc8aedf2ec5f4e7ca079f83.



Here is the part specifically mentioning where the stolen value was transferred:



. . .

Nov-17-2020 12:47:19 AM +UTC

1. The Flash Loan

70,000 ETH was borrowed from dYdX.

2. The Stablecoin Swaps

17,500 ETH was exchanged for 7,855,911.53 USDT on Uniswap.

52,500 ETH was exchanged for 20,987,772.08 DAI on Uniswap.

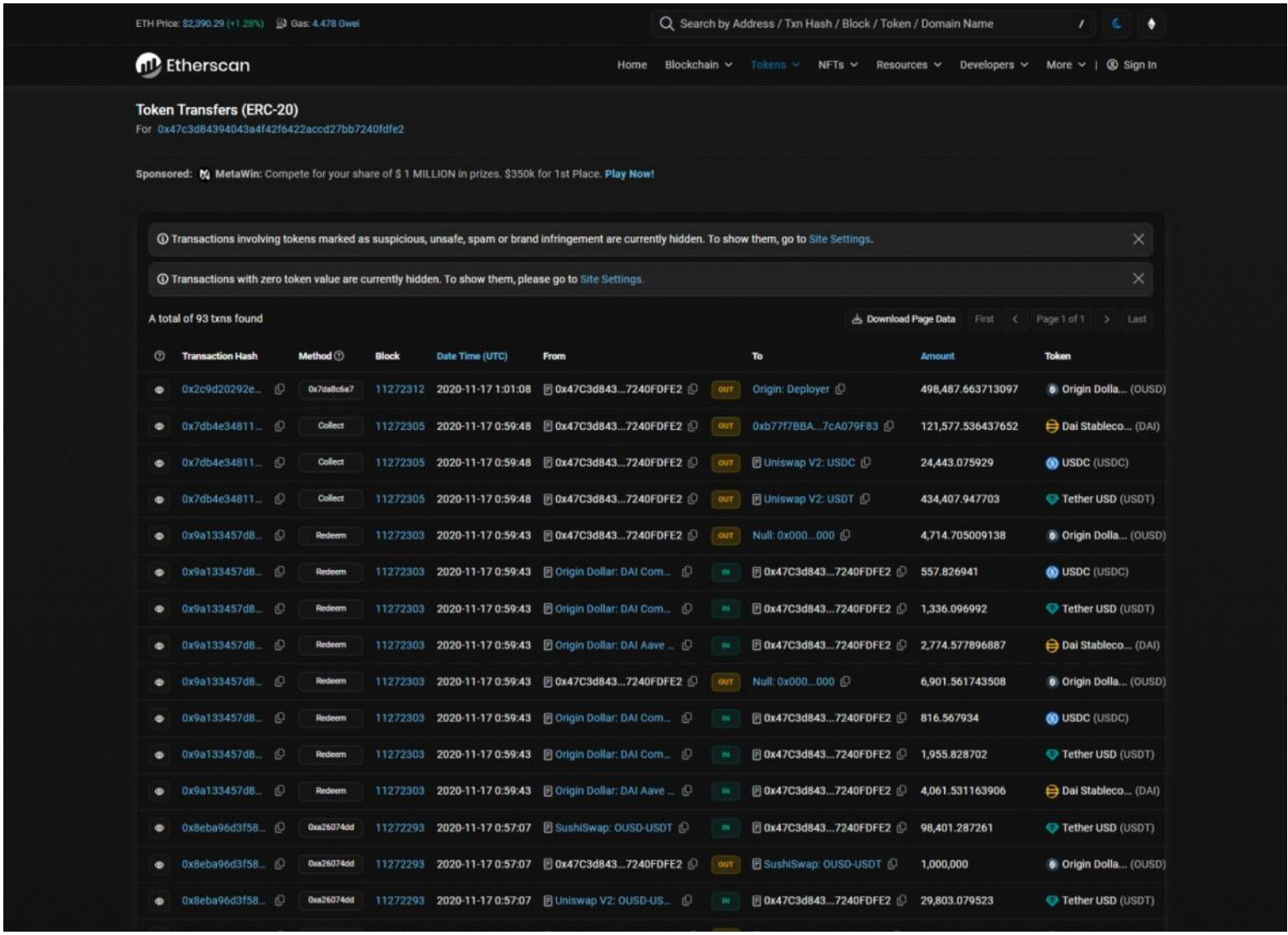
3. The Simple Mint

Our mint method, which allows the sender to use one type of stablecoin to mint OUSD, was called with 7,500,000 USDT.

7,500,000 USDT was transferred to the vault.

7,500,000 OUSD was minted and transferred to the attacker, as intended.

An analysis of the malicious contract shows the attacker manipulating and withdrawing funds from Origin as described in the blog post:



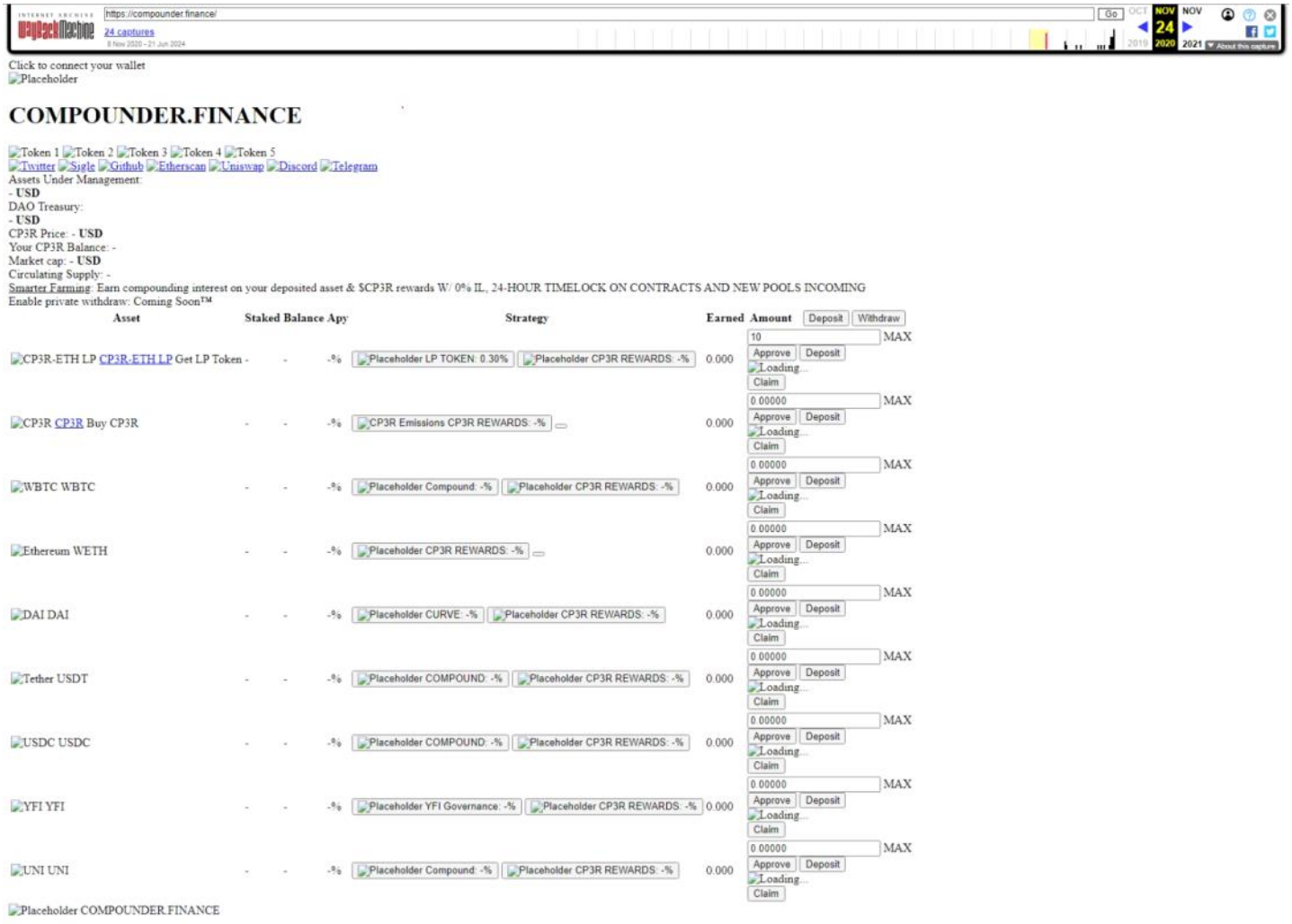
Transaction Hash	Method	Block	Date Time (UTC)	From		To	Amount	Token
0x2c9d20292e...	0x7da8c6a7	11272312	2020-11-17 1:01:08	0x47C3d843...7240FDFE2	OUT	Origin: Deployer	498,487.663713097	Origin Dolla... (OUSD)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	OUT	0xb77f7BBA...7cA079F83	121,577.536437652	Dai Stableco... (DAI)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	OUT	Uniswap V2: USDC	24,443.075929	USDC (USDC)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	OUT	Uniswap V2: USDT	434,407.947703	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	0x47C3d843...7240FDFE2	OUT	Null: 0x000...000	4,714.705009138	Origin Dolla... (OUSD)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	IN	0x47C3d843...7240FDFE2	557.826941	USDC (USDC)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	IN	0x47C3d843...7240FDFE2	1,336.096992	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Aave ...	IN	0x47C3d843...7240FDFE2	2,774.577896887	Dai Stableco... (DAI)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	0x47C3d843...7240FDFE2	OUT	Null: 0x000...000	6,901.561743508	Origin Dolla... (OUSD)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	IN	0x47C3d843...7240FDFE2	816.567934	USDC (USDC)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	IN	0x47C3d843...7240FDFE2	1,955.828702	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Aave ...	IN	0x47C3d843...7240FDFE2	4,061.531163906	Dai Stableco... (DAI)
0x8eba96d3f58...	0xa26074dd	11272293	2020-11-17 0:57:07	SushiSwap: OUSD-USDT	IN	0x47C3d843...7240FDFE2	98,401.287261	Tether USD (USDT)
0x8eba96d3f58...	0xa26074dd	11272293	2020-11-17 0:57:07	0x47C3d843...7240FDFE2	OUT	SushiSwap: OUSD-USDT	1,000,000	Origin Dolla... (OUSD)
0x8eba96d3f58...	0xa26074dd	11272293	2020-11-17 0:57:07	Uniswap V2: OUSD-US...	IN	0x47C3d843...7240FDFE2	29,803.079523	Tether USD (USDT)

Compounder Finance

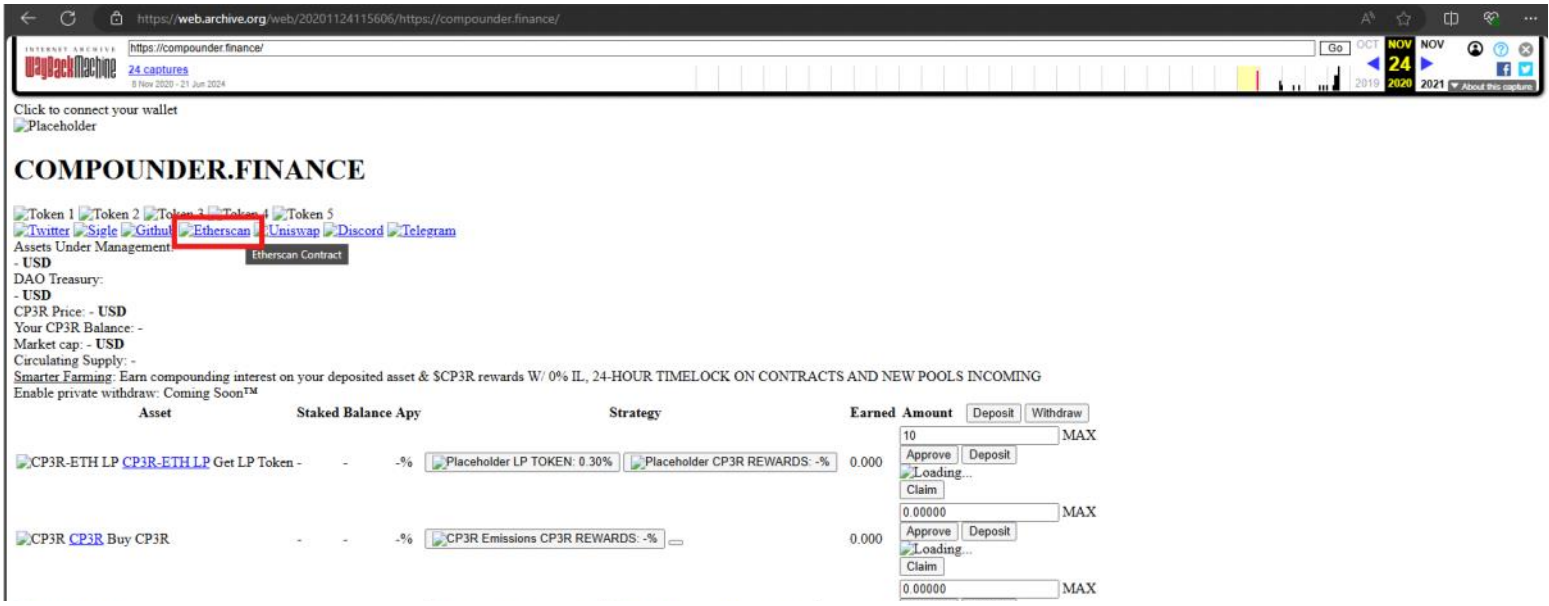
Wednesday, September 11, 2024 10:45 AM

Compounder.finance was a rug pull scam that began on 11/29/2020 that was widely reported in the crypto press.

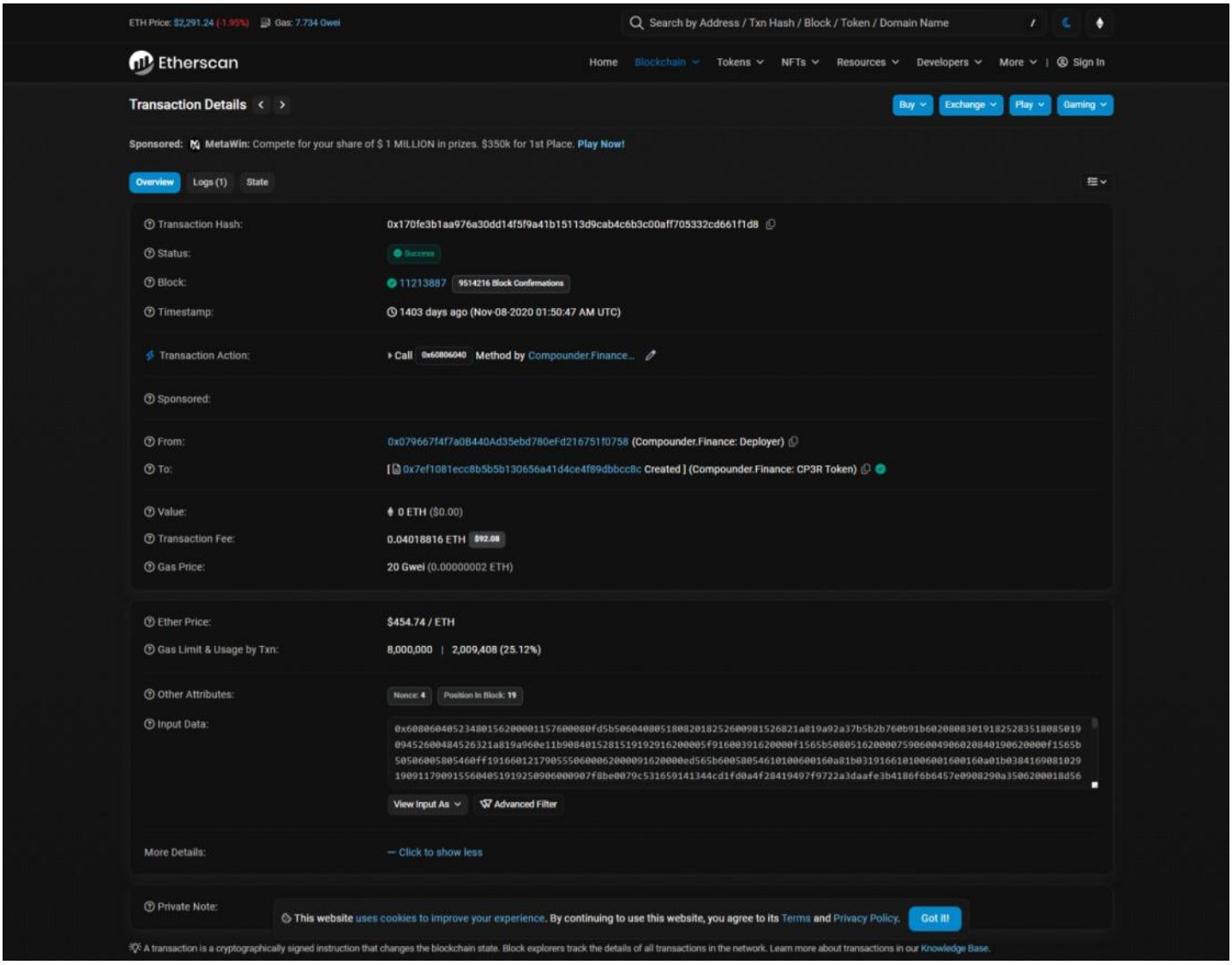
Their website no longer exists, but I found it using archive.org.



The etherscan link on their webpage shows that the compounder.finance Ethereum address is:0x7ef1081ecc8b5b5b130656a41d4ce4f89dbbcc8c



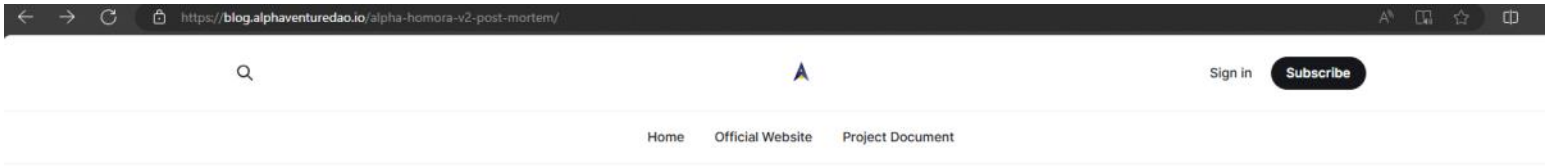
The Compound.Finance contract was deployed by Ethereum address 0x079667f4f7a0B440Ad35ebd780eFd216751f0758 on 11/08/2020 01:50 UTC.



Alpha Homora

Wednesday, September 11, 2024 11:45 AM

On 02/13/2021 05:37 UTC, Alpha Homora DAO was hacked. Later that day, Alpha Homora released a post-mortem on their official website:



HOMORA V2

Alpha Homora V2 Post Mortem

Alpha Homora

Feb 13, 2021 · 5 min

Dear Alpha community, our partners, and DeFi users, as we have shared earlier, we have closed the loophole that made the exploit possible. We'd like to take this opportunity to thank everyone who has helped us, be it on the technical front and non-technical front. We sincerely appreciate it. We are investigating with the relevant parties and will investigate with the authorities to trace the attacker.

Now, we would like to share a post mortem on the recent Alpha Homora V2 exploit to explain

1. What happened

2. Who is affected

3. What's next and

4. Walk through of technical analysis of what happened.

This exploit is complicated, involving more than 9 transactions. We hope this thorough post mortem will not only be helpful to the Alpha community and our partners, but also to other projects and builders in DeFi.

This moment shows how important it is to continue helping each other out and building a safer DeFi ecosystem for everyone. Alpha team is committed to building and helping builders in the space to create a stronger and safer DeFi ecosystem.

What happened?

On Feb 13 5:37AM UTC, an attacker exploited Alpha Homora V2 using a series of complex transactions, which involved flashloans.

Here's what the attacker need to know about the code and the setup in order to execute the attack:

This blog post lays out a walkthrough and technical analysis of the exploit:

Walk through of technical analysis

- Attacker address: 0x905315602ed9a854e325f692ff82f58799beab57
- Attacker's txs: https://etherscan.io/txs?a=0x905315602ed9a854e325f692ff82f58799beab57
- Evil spell address: https://etherscan.io/address/0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2

Exploit Analysis

1.The attacker created an evil spell (can think of this as equivalent to Yearn's strategy). https://etherscan.io/tx/0x2b419173c1f116e94e43afed15a46e3b3a109e118aba166fcca0ba583f686d23

2. Attacker swaps ETH -> UNI, and supply ETH + UNI to Uniswap pool (obtaining ETH/UNI LP token). In the same tx, swap ETH -> sUSD on Uniswap and deposit sUSD

https://blog.alphaventuredao.io/alpha-homora-v2-post-mortem/

Walk through of technical analysis

- Attacker address: 0x905315602ed9a854e325f692ff82f58799beab57
- Attacker's txs: https://etherscan.io/txs?a=0x905315602ed9a854e325f692ff82f58799beab57
- Evil spell address: https://etherscan.io/address/0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2

Exploit Analysis

1.The attacker created an evil spell (can think of this as equivalent to Yearn's strategy). https://etherscan.io/tx/0x2b419173c1f116e94e43afed15a46e3b3a109e118aba166fcca0ba583f686d23

2. Attacker swaps ETH -> UNI, and supply ETH + UNI to Uniswap pool (obtaining ETH/UNI LP token). In the same tx, swap ETH -> sUSD on Uniswap and deposit sUSD to Cream's Iron Bank (getting cysUSD) https://etherscan.io/tx/0x4441eefe434fbef9d9b3acb169e35eb7b3958763b74c5617b39034decd4dd3ad

3. Call execute to HomoraBankV2 using the evil spell (creating position 883), performing:

- Borrow 1000e18 sUSD
- Deposit UNI-WETH LP to WERC20, and use as collateral (to bypass the collateral > borrow check)
- In the process, the attacker has 1000e18 sUSD debt shares (because the attacker is the first borrower)

https://etherscan.io/tx/0xcc57ac77dc3953de7832162ea4cd925970e064ead3f6861ee40076aca8e7e571

4. Call execute to HomoraBankV2 using the evil spell again (to position 883), performing:

- Repay 1000000098548938710983 sUSD (actual debt with interest accrued is 1000000098548938710984 sUSD), resulting in a repay share of 1 less than the total share.
- As a result, the attacker now has 1 minisUSD debt and 1 debt share.

https://etherscan.io/tx/0xf31ee9d9e83db3592601b854fe4f8b872cecd0ea2a3247c475eea8062a20dd41

The blog post also names the attacker's address as 0x905315602ed9a854e325f692ff82f58799beab57.
The malicious contract was 0x560A8E3B79d23b0A525E15C6F3486c6A293DDAd2.

Below are the ERC20 transactions associated with this contract:

ETH Price: $2,322.33 (-0.12%) Gas: 3.931 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Etherscan

Home Blockchain Tokens NFTs Resources Developers More Sign In

Token Transfers (ERC-20)

For 0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2

Sponsored: Maker is now Sky. Get rewarded for saving without giving up control.

Transactions involving tokens marked as suspicious, unsafe, spam or brand infringement are currently hidden. To show them, go to Site Settings.

Transactions with zero token value are currently hidden. To show them, please go to Site Settings.

A total of 139 txns found

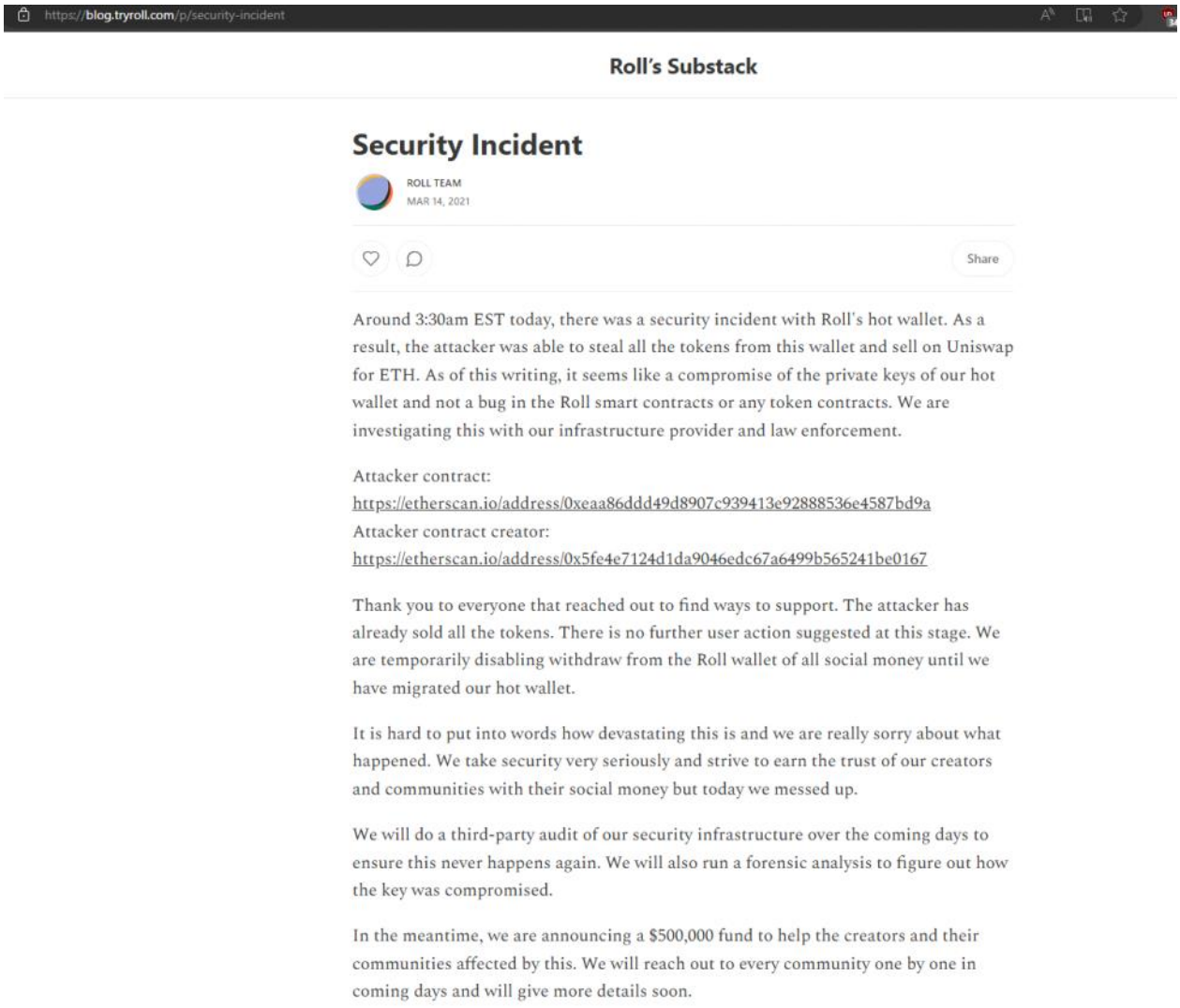
Download Page Data First Page 2 of 2 Last

Transaction Hash	Method	Block	Date Time (UTC)	From		To	Amount	Token
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	Cream.Finance: cySUS...	IN	0x560A8E3B...A293DDAd2	131,885.08558758	Yearn Synth ... (cySUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x560A8E3B...A293DDAd2	OUT	Cream.Finance: cySUS...	1,321.409764412	Synth sUSD (sUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x5f5Cd910...Cd00457bb	IN	0x560A8E3B...A293DDAd2	661.350732531	Synth sUSD (sUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x5f5Cd910...Cd00457bb	IN	0x560A8E3B...A293DDAd2	330.675366265	Synth sUSD (sUSD)

Try Roll

Wednesday, September 11, 2024 12:19 PM

On March 14, 2021, Try Roll posted on their website a blog post titled "Security Incident" that stated unknown attacker was able to gain access to the private keys of Tryroll's hot wallet. The stated that the malicious contract was 0xeaa86ddd49d8907c939413e92888536e4587bd9a and the malicious contract creator was 0x5fe4e7124d1da9046edc67a6499b565241be0167.



https://blog.tryroll.com/p/security-incident

Roll's Substack

Security Incident

ROLL TEAM
MAR 14, 2021

Share

Around 3:30am EST today, there was a security incident with Roll's hot wallet. As a result, the attacker was able to steal all the tokens from this wallet and sell on Uniswap for ETH. As of this writing, it seems like a compromise of the private keys of our hot wallet and not a bug in the Roll smart contracts or any token contracts. We are investigating this with our infrastructure provider and law enforcement.

Attacker contract:
https://etherscan.io/address/0xeaa86ddd49d8907c939413e92888536e4587bd9a
Attacker contract creator:
https://etherscan.io/address/0x5fe4e7124d1da9046edc67a6499b565241be0167

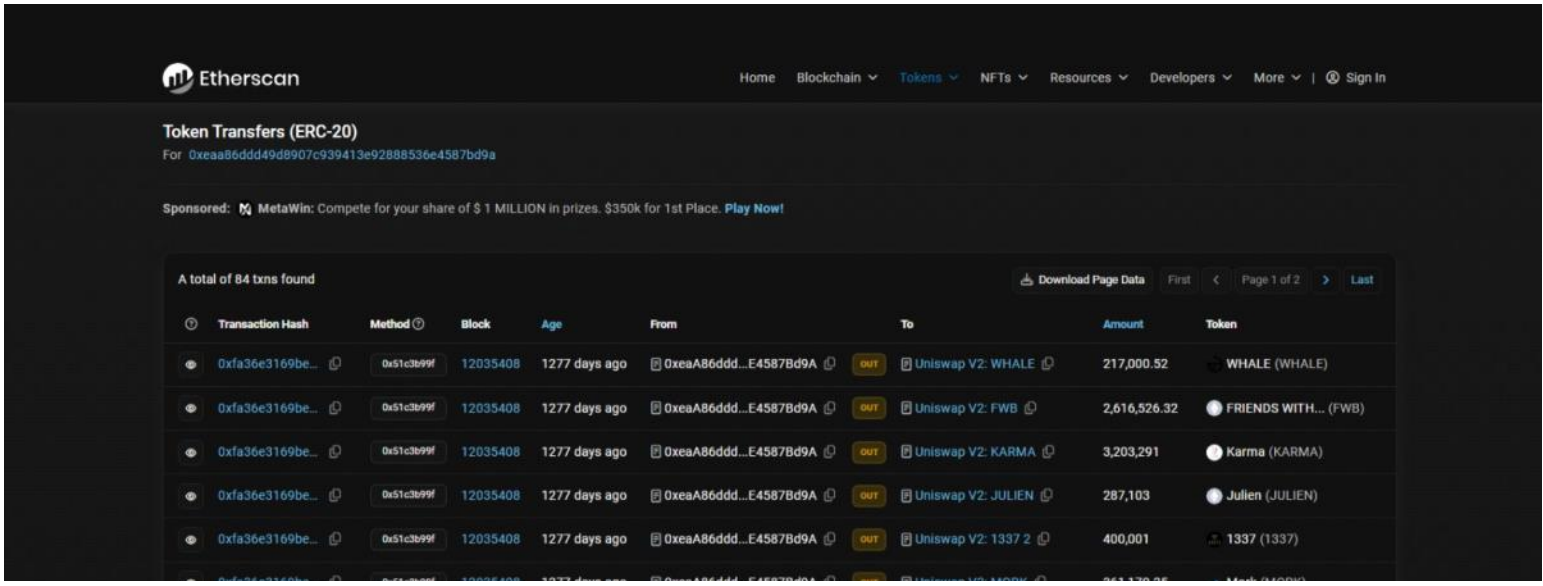
Thank you to everyone that reached out to find ways to support. The attacker has already sold all the tokens. There is no further user action suggested at this stage. We are temporarily disabling withdraw from the Roll wallet of all social money until we have migrated our hot wallet.

It is hard to put into words how devastating this is and we are really sorry about what happened. We take security very seriously and strive to earn the trust of our creators and communities with their social money but today we messed up.

We will do a third-party audit of our security infrastructure over the coming days to ensure this never happens again. We will also run a forensic analysis to figure out how the key was compromised.

In the meantime, we are announcing a $500,000 fund to help the creators and their communities affected by this. We will reach out to every community one by one in coming days and will give more details soon.

An analysis of the malicious contract, shows the ERC20 tokens transferred from the hot wallet and swapped for Ether:



Etherscan

Home Blockchain Tokens NFTs Resources Developers More | Sign In

Token Transfers (ERC-20)
For 0xeaa86ddd49d8907c939413e92888536e4587bd9a

Sponsored: MetaWin: Compete for your share of $ 1 MILLION in prizes. $350k for 1st Place. Play Now!

A total of 84 txns found

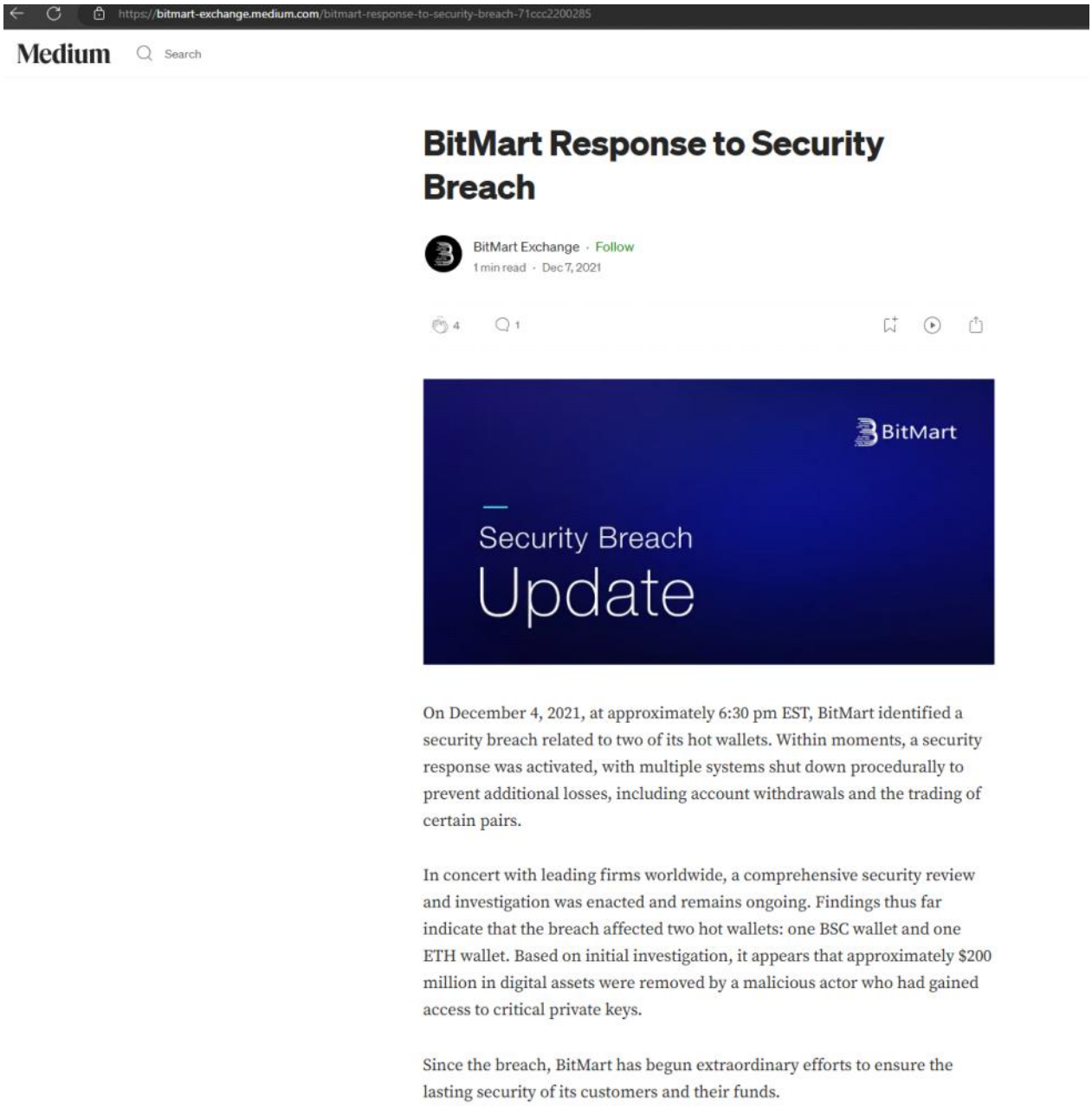
Download Page Data First Page 1 of 2 Last

Transaction Hash	Method	Block	Age	From		To	Amount	Token
0xfa36e3169be...	0x51c3b99f	12035408	1277 days ago	0xeaA86ddd...E4587Bd9A	OUT	Uniswap V2: WHALE	217,000.52	WHALE (WHALE)
0xfa36e3169be...	0x51c3b99f	12035408	1277 days ago	0xeaA86ddd...E4587Bd9A	OUT	Uniswap V2: FWB	2,616,526.32	FRIENDS WITH... (FWB)
0xfa36e3169be...	0x51c3b99f	12035408	1277 days ago	0xeaA86ddd...E4587Bd9A	OUT	Uniswap V2: KARMA	3,203,291	Karma (KARMA)
0xfa36e3169be...	0x51c3b99f	12035408	1277 days ago	0xeaA86ddd...E4587Bd9A	OUT	Uniswap V2: JULIEN	287,103	Julien (JULIEN)
0xfa36e3169be...	0x51c3b99f	12035408	1277 days ago	0xeaA86ddd...E4587Bd9A	OUT	Uniswap V2: 1337 2	400,001	1337 (1337)

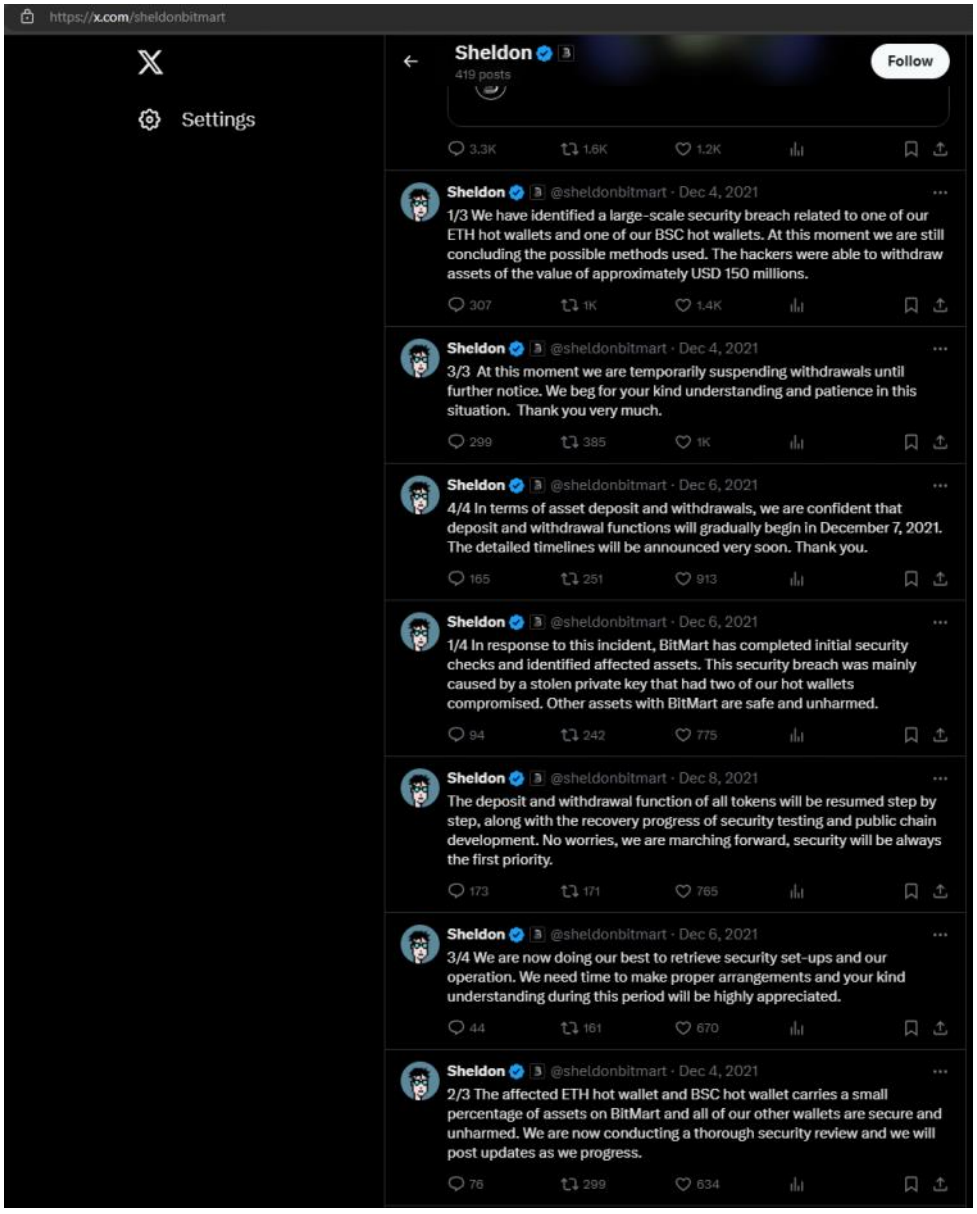
Bitmart

Wednesday, September 11, 2024 1:08 PM

On December 7, 2021, exchange Bitmart announced on their official blog that there was a security incident where an actor stole private keys for their BSC and ETH hot wallets. The incident happened on December 4, 2021 and resulted in an approximate loss of $200 million.

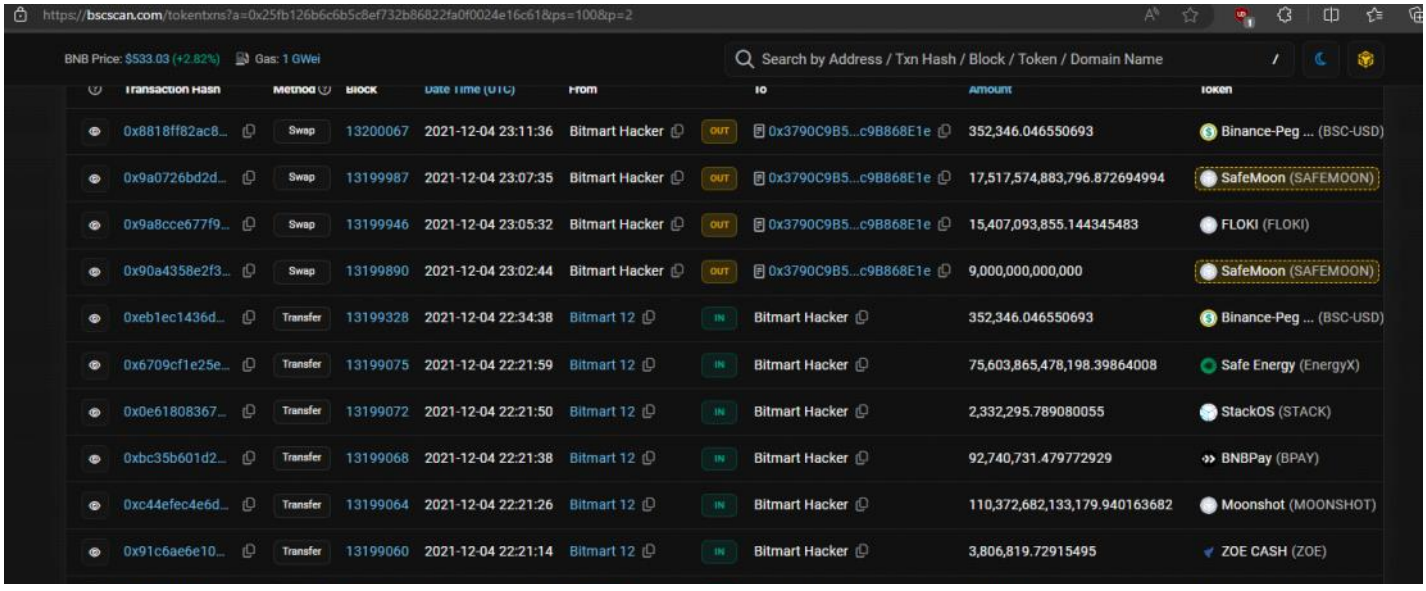


Bitmart's CEO Sheldon Xia also release a series of tweets describing the incident:



An analysis of Bitmart's ETH and BSC hot wallets on 12/04/2021 shows large outflows or ERC20 tokens to Ethereum attacker wallet 0x39fB0dCd13945B835d47410Ae0DE7181D3edf270 and Binance Smart Chain attacker wallet 0x25fb126b6c6b5c8ef732b86822fa0f0024e16c61.

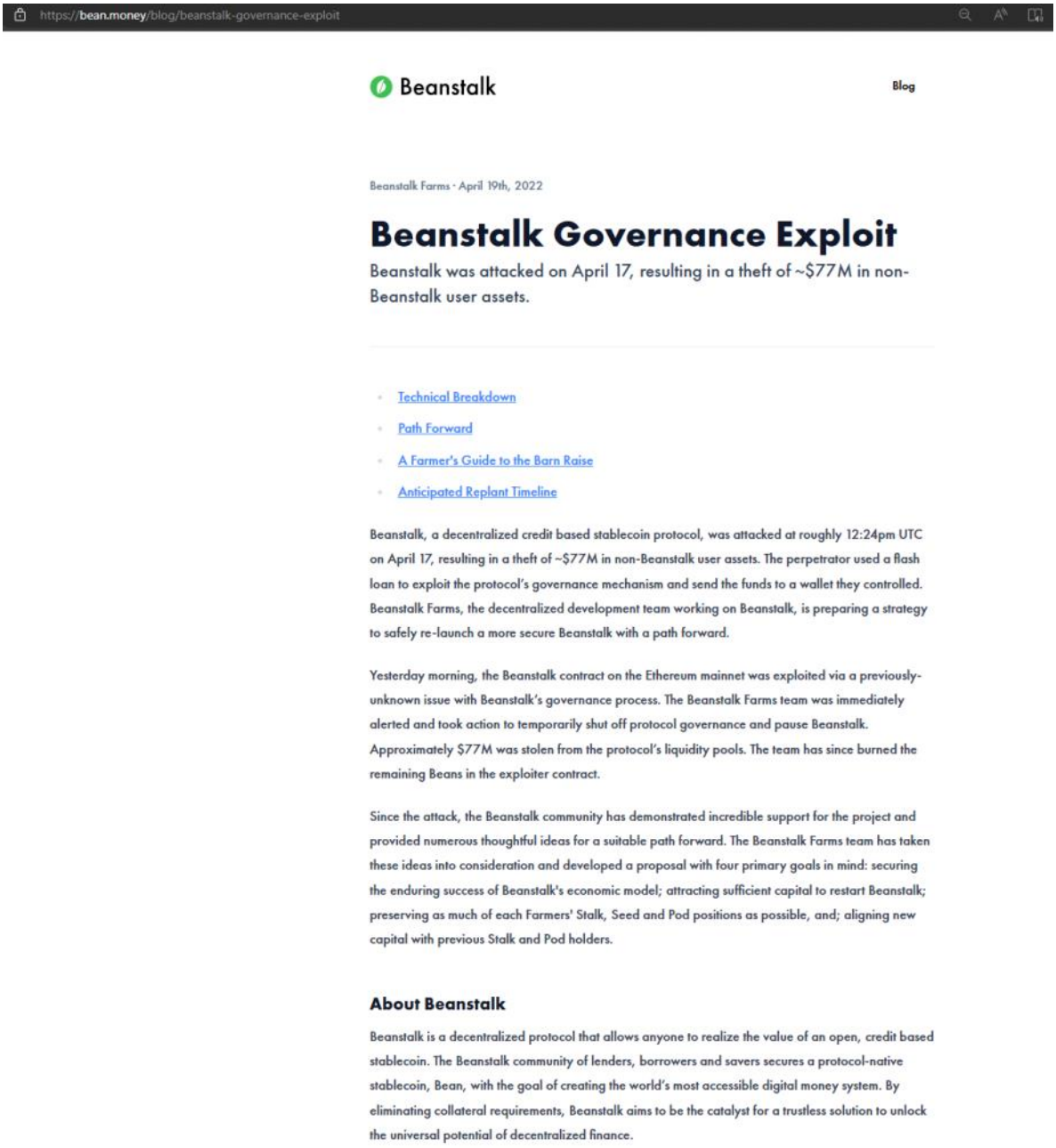
Here are BSC token transfers showing the Bitmart hacker stealing tokens from the Bitmart BSC smart chain:



Beanstalk

Wednesday, September 11, 2024 4:23 PM

04/19/2022, Beanstalk released a statement on their official blog explaining that on 04/17/2022 at approximately 12:24 UTC approximately $77 million was stolen using an exploit in the Beanstalk protocol.



https://bean.money/blog/beanstalk-governance-exploit

Beanstalk Blog

Beanstalk Farms · April 19th, 2022

Beanstalk Governance Exploit

Beanstalk was attacked on April 17, resulting in a theft of ~$77M in non-Beanstalk user assets.

- Technical Breakdown
- Path Forward
- A Farmer's Guide to the Barn Raise
- Anticipated Replant Timeline

Beanstalk, a decentralized credit based stablecoin protocol, was attacked at roughly 12:24pm UTC on April 17, resulting in a theft of ~$77M in non-Beanstalk user assets. The perpetrator used a flash loan to exploit the protocol's governance mechanism and send the funds to a wallet they controlled. Beanstalk Farms, the decentralized development team working on Beanstalk, is preparing a strategy to safely re-launch a more secure Beanstalk with a path forward.

Yesterday morning, the Beanstalk contract on the Ethereum mainnet was exploited via a previously-unknown issue with Beanstalk's governance process. The Beanstalk Farms team was immediately alerted and took action to temporarily shut off protocol governance and pause Beanstalk. Approximately $77M was stolen from the protocol's liquidity pools. The team has since burned the remaining Beans in the exploiter contract.

Since the attack, the Beanstalk community has demonstrated incredible support for the project and provided numerous thoughtful ideas for a suitable path forward. The Beanstalk Farms team has taken these ideas into consideration and developed a proposal with four primary goals in mind: securing the enduring success of Beanstalk's economic model; attracting sufficient capital to restart Beanstalk; preserving as much of each Farmers' Stalk, Seed and Pod positions as possible, and; aligning new capital with previous Stalk and Pod holders.

About Beanstalk

Beanstalk is a decentralized protocol that allows anyone to realize the value of an open, credit based stablecoin. The Beanstalk community of lenders, borrowers and savers secures a protocol-native stablecoin, Bean, with the goal of creating the world's most accessible digital money system. By eliminating collateral requirements, Beanstalk aims to be the catalyst for a trustless solution to unlock the universal potential of decentralized finance.

The "Technical Breakdown" link leads to a blog post on Medium.com titled "Beanstalk $BEAN Exploit". In this article, specific technical details about the exploit are explained. This article states that the attacker's Ethereum address was 0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4.

Secondly, approximately nine minutes later, the same address deposited the 212,858 BEAN into the Beanstalk Silo (https://etherscan.io/tx/0xf5a698984485d01e09744e8d7b8ca15cd29aa430a0137349c8c9e19e60c0bb9d)

Thirdly, since a proportionate amount of *Stalk* is immediately generated upon a whitelisted asset deposit, this Silo deposit allowed the address to propose Beanstalk Improvement Proposals (BIP) 18 (https://etherscan.io/tx/0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f/advanced) and 19 (https://etherscan.io/tx/0x9575e478d7c542558ecca52b27072fa1f1ec70679106bdbd62f3bb4d6c87a80d).

BIP-18 was originally left blank, and BIP-19 (exploiter named it InitBip18, we'll get to that later) contained a verified contract that proposed a $250k donation to the Ukraine wallet address, as well as $10k to the proposer.

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.13;

// Ukraine Donation Proposal
// Give 250,000 Bean to Ukraine (and 10,000 Bean to the proposer)

abstract contract IBean {
    function mint(address account, uint256 amount) public virtual returns (bool);
}

contract InitBip18 {
    address private constant bean = 0xDC59ac4FeFa32293A95889Dc396682858d52e5Db; // Bean Address
    address private constant proposerWallet = 0xE5eCF73603D98A0128F05ed30506ac7A663dBb69; // Proposer Wallet
    address private constant ukraineWallet = 0x165CD37b4C644C2921454429E7F9358d18A45e14; // Ukraine Wallet
    uint256 private constant proposerAmount = 10_000 * 1e6; // 10,000 Beans
    uint256 private constant donationAmount = 250_000 * 1e6; // 250,000 Beans

    function init() external {
        IBean(bean).mint(proposerWallet, proposerAmount);
        IBean(bean).mint(ukraineWallet, donationAmount);
    }
}
```

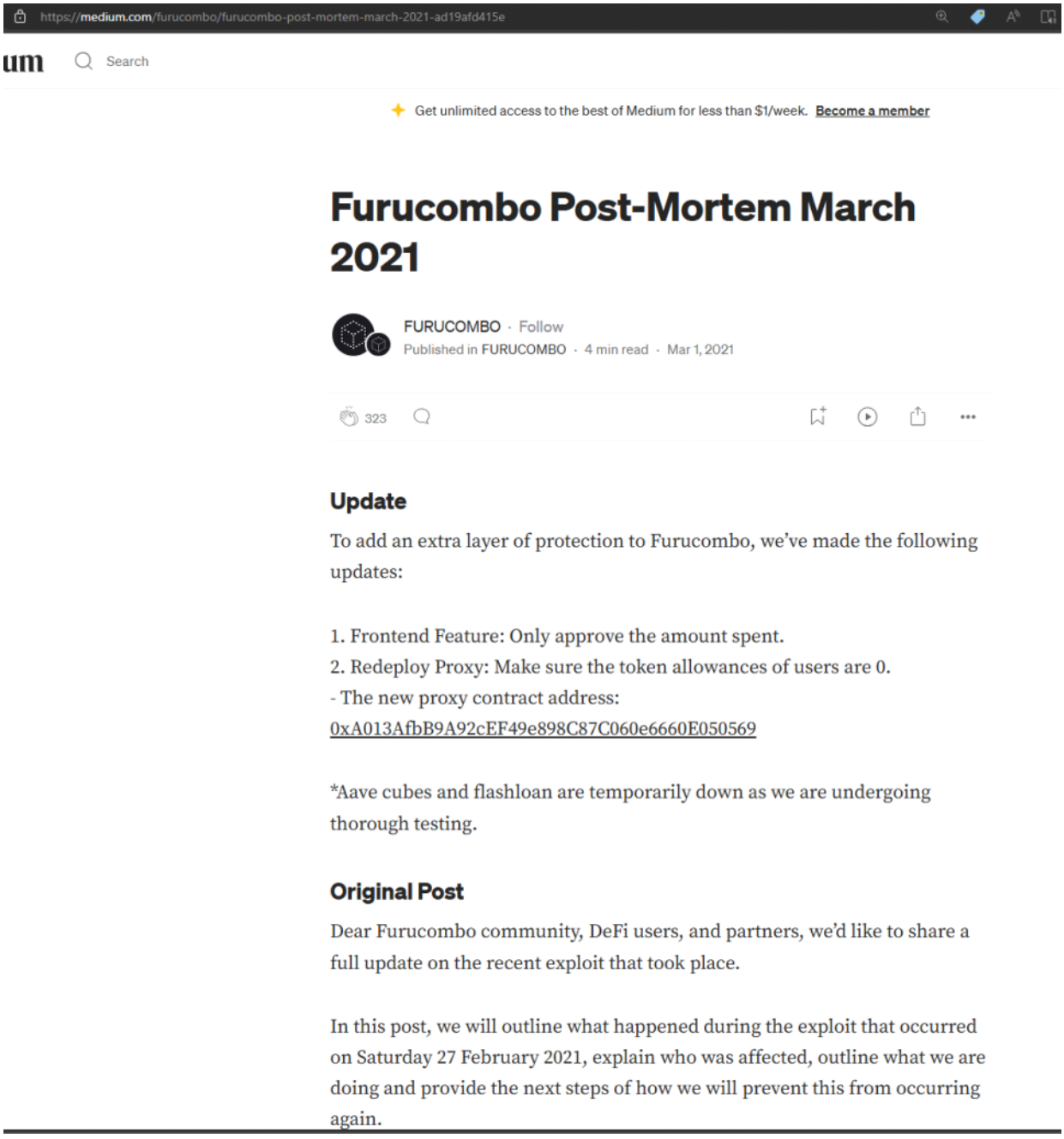
Source: https://etherscan.io/address/0x259a2795624b8a17bc7eb312a94504ad0f615d1e#code

An analysis of this address shows the attacker stealing approximately 24,830 ETH as described in the technical breakdown:

Furucombo

Wednesday, September 11, 2024 4:59 PM

On 02/27/2021, DeFI platform Furucombo was exploited and approximately $15 million was stolen.
Furucombo announced this exploit on their official blog:



https://medium.com/furucombo/furucombo-post-mortem-march-2021-ad19afd415e

um Search

Get unlimited access to the best of Medium for less than $1/week. Become a member

Furucombo Post-Mortem March 2021

FURUCOMBO · Follow
Published in FURUCOMBO · 4 min read · Mar 1, 2021

323

Update

To add an extra layer of protection to Furucombo, we've made the following updates:

1. Frontend Feature: Only approve the amount spent.
2. Redeploy Proxy: Make sure the token allowances of users are 0.
- The new proxy contract address:
0xA013AfbB9A92cEF49e898C87C060e6660E050569

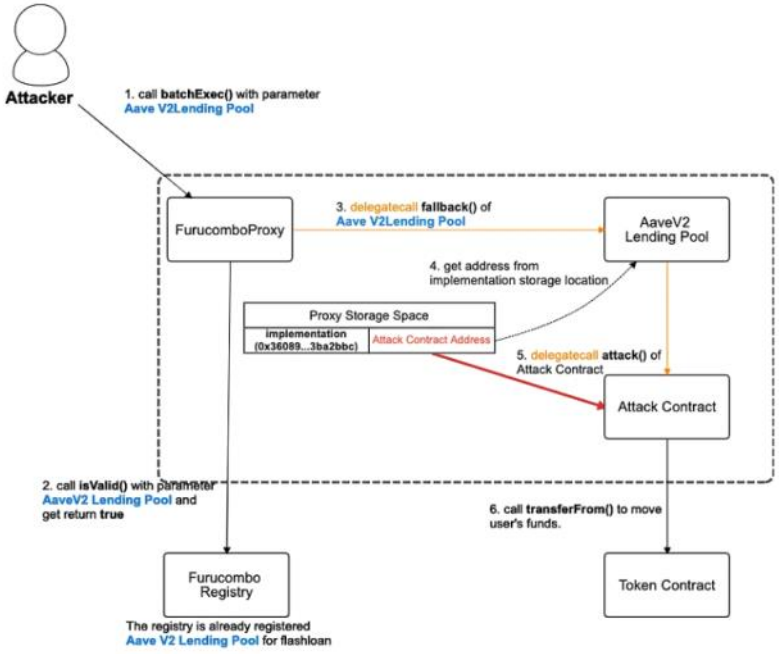
*Aave cubes and flashloan are temporarily down as we are undergoing thorough testing.

Original Post

Dear Furucombo community, DeFi users, and partners, we'd like to share a full update on the recent exploit that took place.

In this post, we will outline what happened during the exploit that occurred on Saturday 27 February 2021, explain who was affected, outline what we are doing and provide the next steps of how we will prevent this from occurring again.

The technical section of this blog post revealed a transaction associated with the hacker:
0xfaf46447572617a7eef027be43525b3168e4b650c07a50338faa453dda1f1940



After the compromise was discovered, we immediately removed the Aave v2 lending pool from the registry contract at 05:46:16 PM UTC, as this was the key element of the attack. The attacker's transaction at 05:55:17 PM UTC was then reverted [4]. Though the handler was not affected, we temporarily paused the function of Aave cubes. The rest of the cubes remain functional.

. . .

Links

- Website: furucombo.app
- Discord: discord.furucombo.app
- Forum: forum.furucombo.app

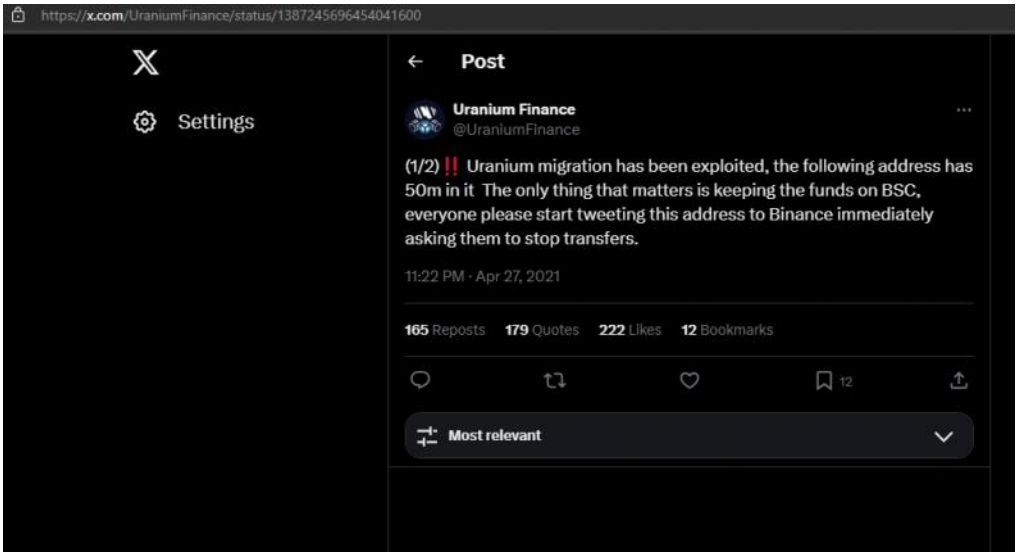
https://etherscan.io/tx/0xfaf46447572617a7eef027be43525b3168e4b650c07a50338faa453dda1f1940

An analysis of this transaction shows that the hacker's wallet is:
0xb624E2b10b84a41687caeC94BDd484E48d76B212

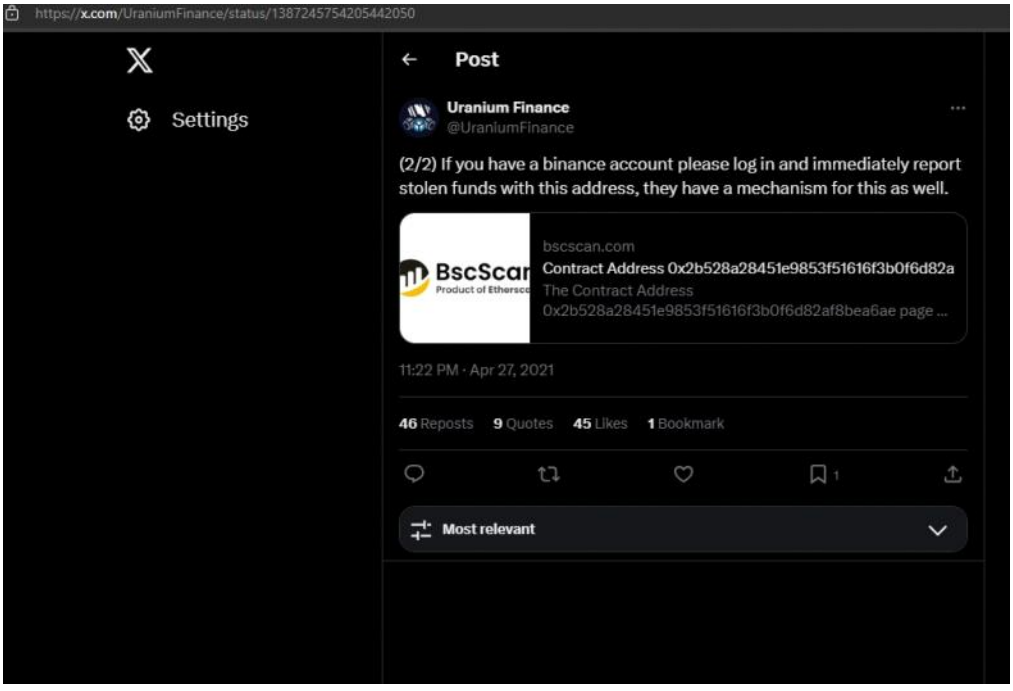
Uranium Finance

Wednesday, September 11, 2024 5:54 PM

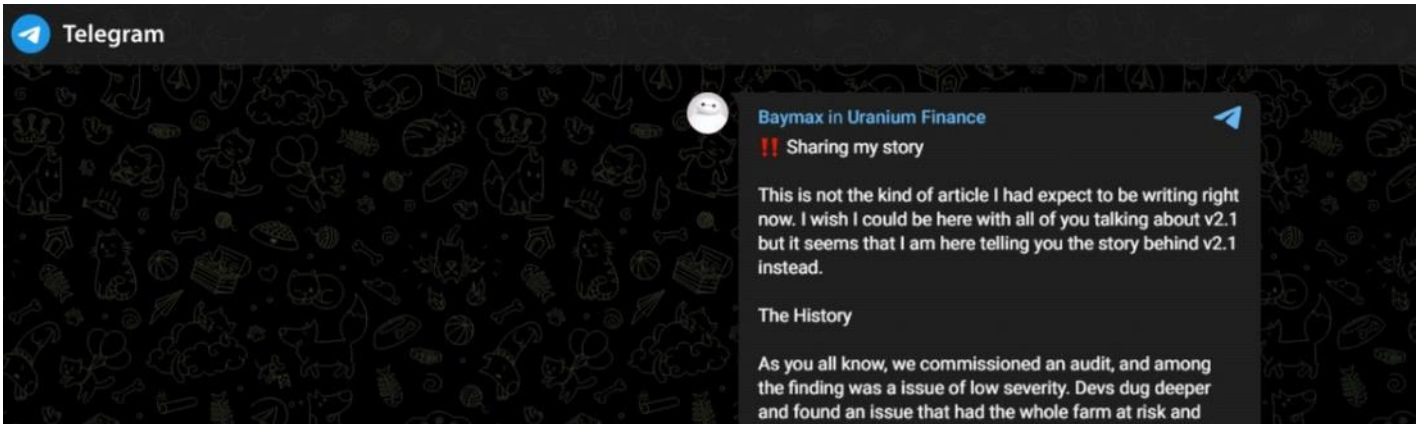
On 04/27/2021 the official Uranium Finance Twitter account tweeted that their protocol had been exploited:

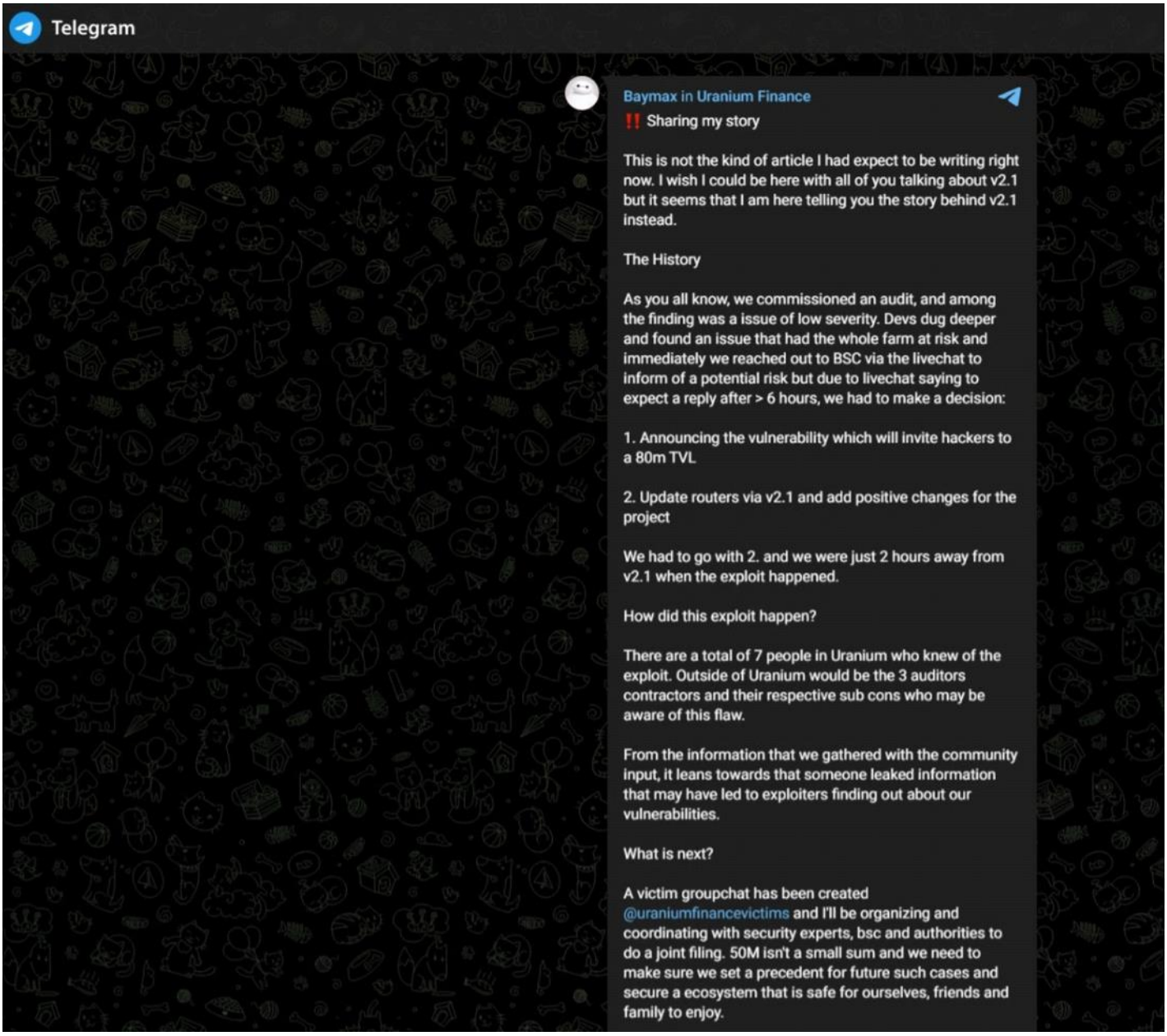


They sent a second tweet stating the contract address of the hacker:

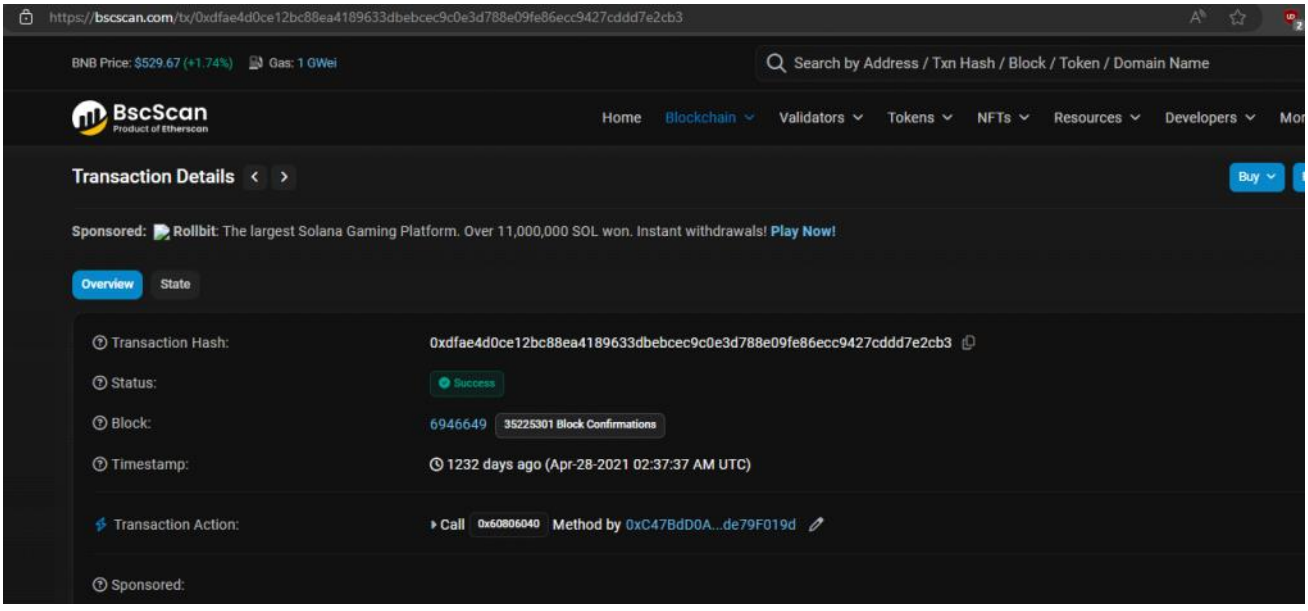


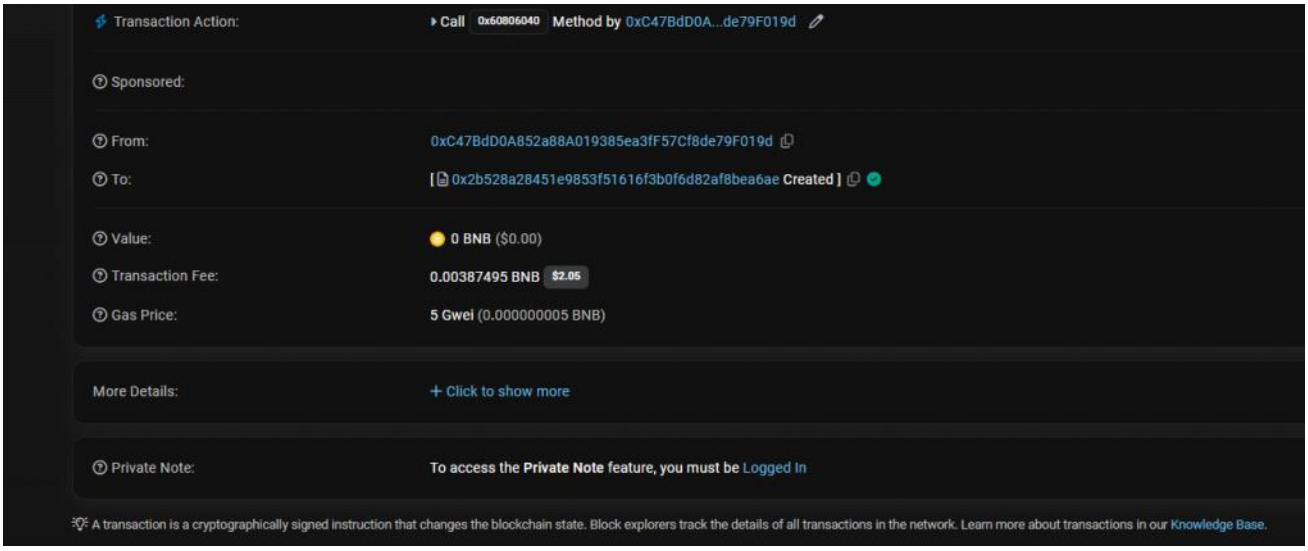
On 04/28/2021, in a post to their Telegram channel, Uranium Finance described how the exploit worked:



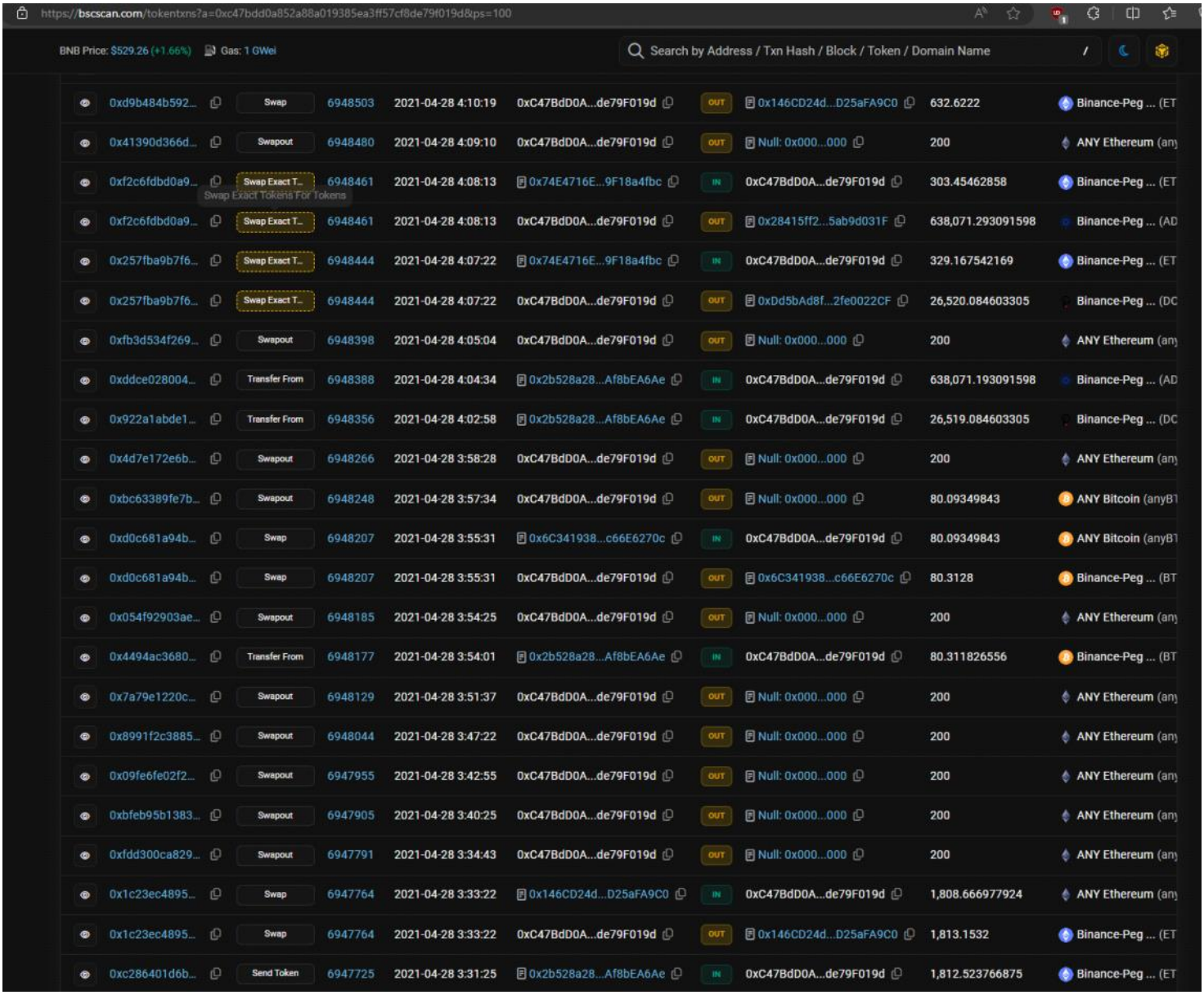


An analysis of the malicious contract shows that its creator was 0xC47BdD0A852a88A019385ea3fF57Cf8de79F019d:





An analysis of the token transactions in this account shows the tokens being stolen on 04/28/2021:



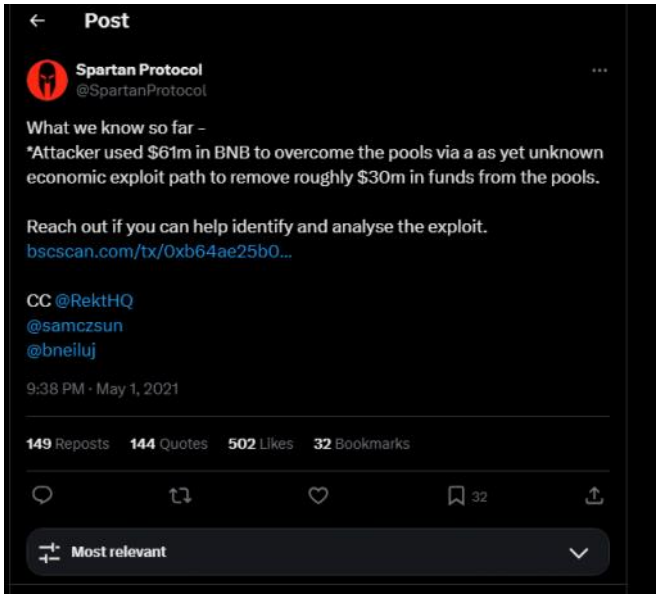
Shortly thereafter, the hacker swaps the stolen tokens for ETH sent to address 0xc61429117038A1f13881DD7410B80771F28e06ec.

0xfdd300ca82956b6440ce7f13c0aa0d4868a2772063ab5b58bd4e547853248bfd

Spartan Protocol

Wednesday, September 11, 2024 6:36 PM

On 05/01/2021, the official Spartan Protocol Twitter account announced they had been hacked and the hackers BSC address was 0x3B6e77722e2bBe97C1cfA337B42C0939AEb83671.

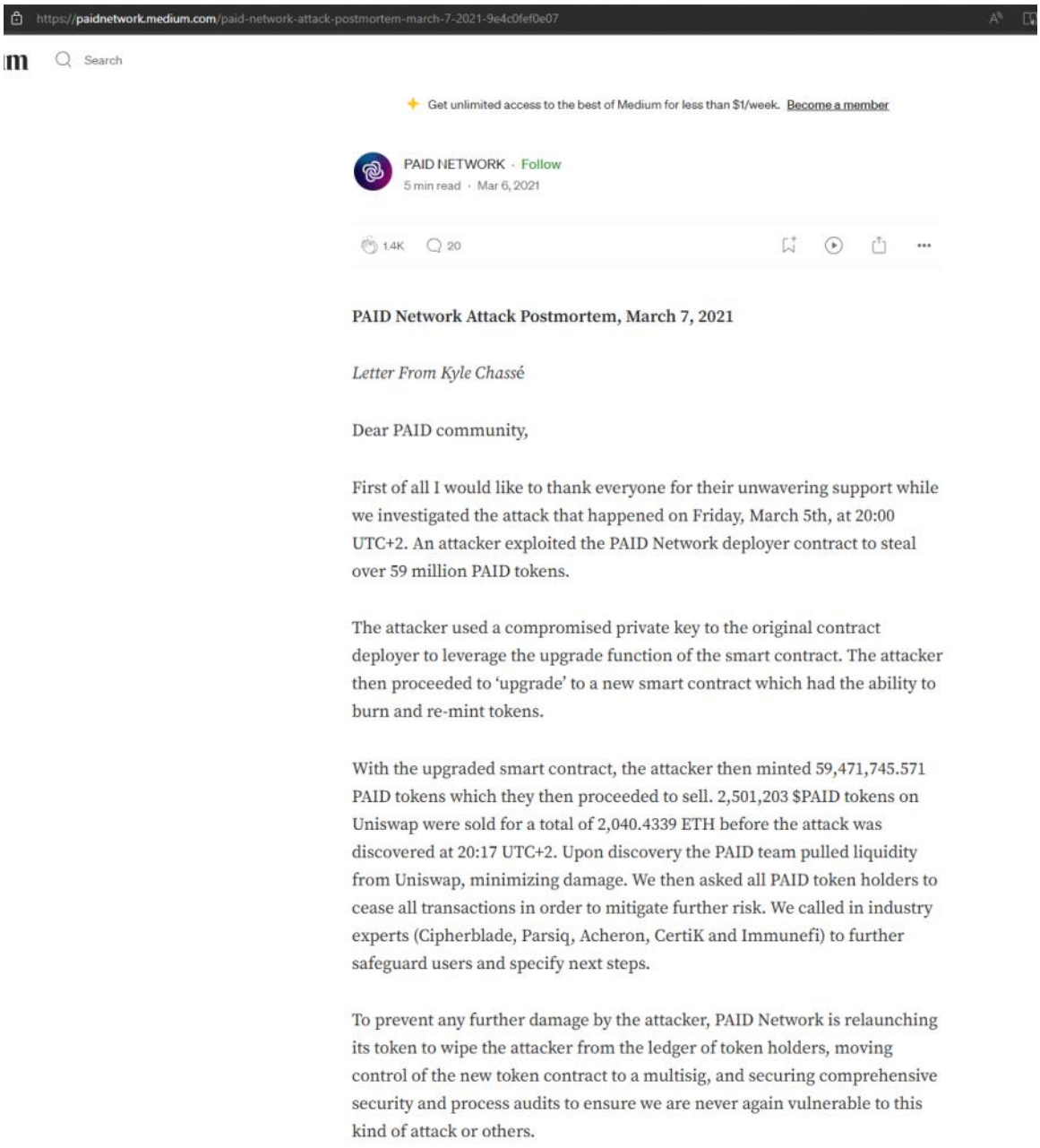


An analysis of token transfers of this address show the hacker executing the heist:

PAID Network

Thursday, September 12, 2024 10:28 AM

On 3/7/2021, PAID Network published a postmortem on their Medium.com account stating that they were hacked on 03/05/2021 at 18:00 UTC. Specifically, the attacker used stolen private keys to steal approximately 59.48 million PAID tokens.



https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

Search

Get unlimited access to the best of Medium for less than $1/week. Become a member

PAID NETWORK · Follow
5 min read · Mar 6, 2021

1.4K 20

PAID Network Attack Postmortem, March 7, 2021

Letter From Kyle Chassé

Dear PAID community,

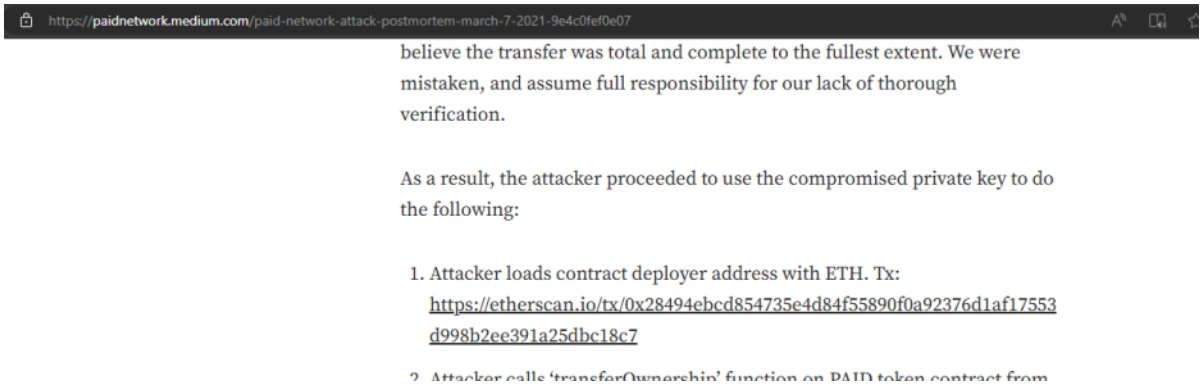
First of all I would like to thank everyone for their unwavering support while we investigated the attack that happened on Friday, March 5th, at 20:00 UTC+2. An attacker exploited the PAID Network deployer contract to steal over 59 million PAID tokens.

The attacker used a compromised private key to the original contract deployer to leverage the upgrade function of the smart contract. The attacker then proceeded to 'upgrade' to a new smart contract which had the ability to burn and re-mint tokens.

With the upgraded smart contract, the attacker then minted 59,471,745.571 PAID tokens which they then proceeded to sell. 2,501,203 $PAID tokens on Uniswap were sold for a total of 2,040.4339 ETH before the attack was discovered at 20:17 UTC+2. Upon discovery the PAID team pulled liquidity from Uniswap, minimizing damage. We then asked all PAID token holders to cease all transactions in order to mitigate further risk. We called in industry experts (Cipherblade, Parsiq, Acheron, CertiK and Immunefi) to further safeguard users and specify next steps.

To prevent any further damage by the attacker, PAID Network is relaunching its token to wipe the attacker from the ledger of token holders, moving control of the new token contract to a multisig, and securing comprehensive security and process audits to ensure we are never again vulnerable to this kind of attack or others.

This blog further details in the "Technical Analysis of the Attack" section that the transaction hash of 0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0 shows where the attacker sends the stolen PAID coin to his Ethereum address.



https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

believe the transfer was total and complete to the fullest extent. We were mistaken, and assume full responsibility for our lack of thorough verification.

As a result, the attacker proceeded to use the compromised private key to do the following:

1. Attacker loads contract deployer address with ETH. Tx: https://etherscan.io/tx/0x28494ebcd854735e4d84f55890f0a92376d1af17553d998b2ee391a25dbc18c7

2. Attacker calls 'transferOwnership' function on PAID token contract from

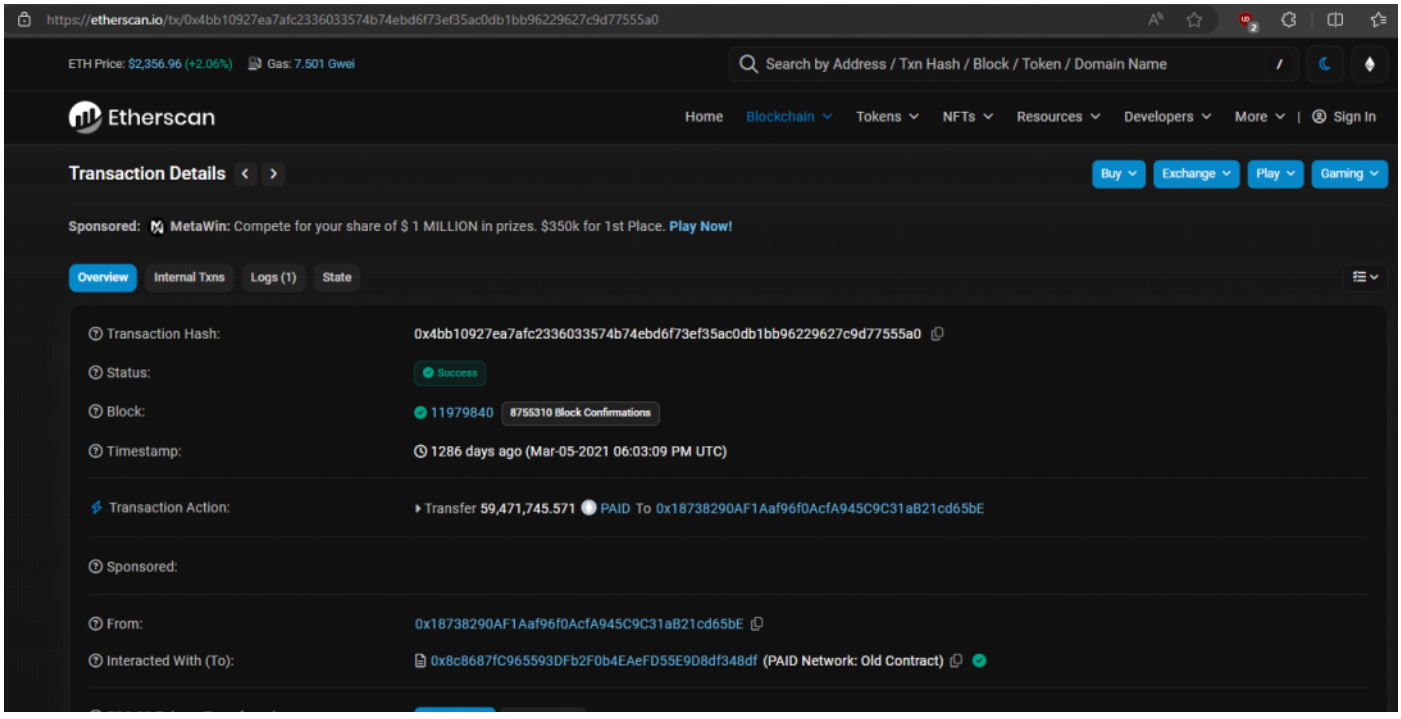
https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

believe the transfer was total and complete to the fullest extent. We were mistaken, and assume full responsibility for our lack of thorough verification.

As a result, the attacker proceeded to use the compromised private key to do the following:

1. Attacker loads contract deployer address with ETH. Tx: https://etherscan.io/tx/0x28494ebcd854735e4d84f55890f0a92376d1af17553d998b2ee391a25dbc18c7
2. Attacker calls 'transferOwnership' function on PAID token contract from PAID deployer address. Tx: https://etherscan.io/tx/0x733dd279b3d24f3415f3850b8eceafc651c1998163dcd0352b9e83c46e2b33d9
3. Attacker deploys a new contract. Tx: https://etherscan.io/tx/0xfe6eb5800741e986d6375d8e3f94eefd00cc64ba8896389142fdb6162a34d9b8
4. Attackers burns PAID tokens on the staking rewards address. Tx: https://etherscan.io/tx/0x3a483dd881d98541ebbd51e9a64daa700546bae9c2b33a30c2192f9981334b9b
5. Attacker mints 59,471,745.571 tokens, which he sends to his address. Tx: https://etherscan.io/tx/0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0
6. Attacker approves trading on Uniswap for his address. Tx: https://etherscan.io/tx/0x1a23506c2a53e9811ebe7ab9d78ba1ab9e02766d2440ff152437a3176a314a38
7. Attacker proceeds to sell 2,501,203 $PAID tokens on Uniswap for a total of 2,040.4339 ETH before being stopped by the PAID Network team's efforts to pull Uniswap liquidity. All funds (PAID and ETH) remain at the attacker's address, found here: https://etherscan.io/address/0x18738290af1aaf96f0acfa945c9c31ab21cd65be

An analysis of that transaction shows that the attacker's address is 0x18738290AF1Aaf96f0AcfA945C9C31aB21cd65bE:

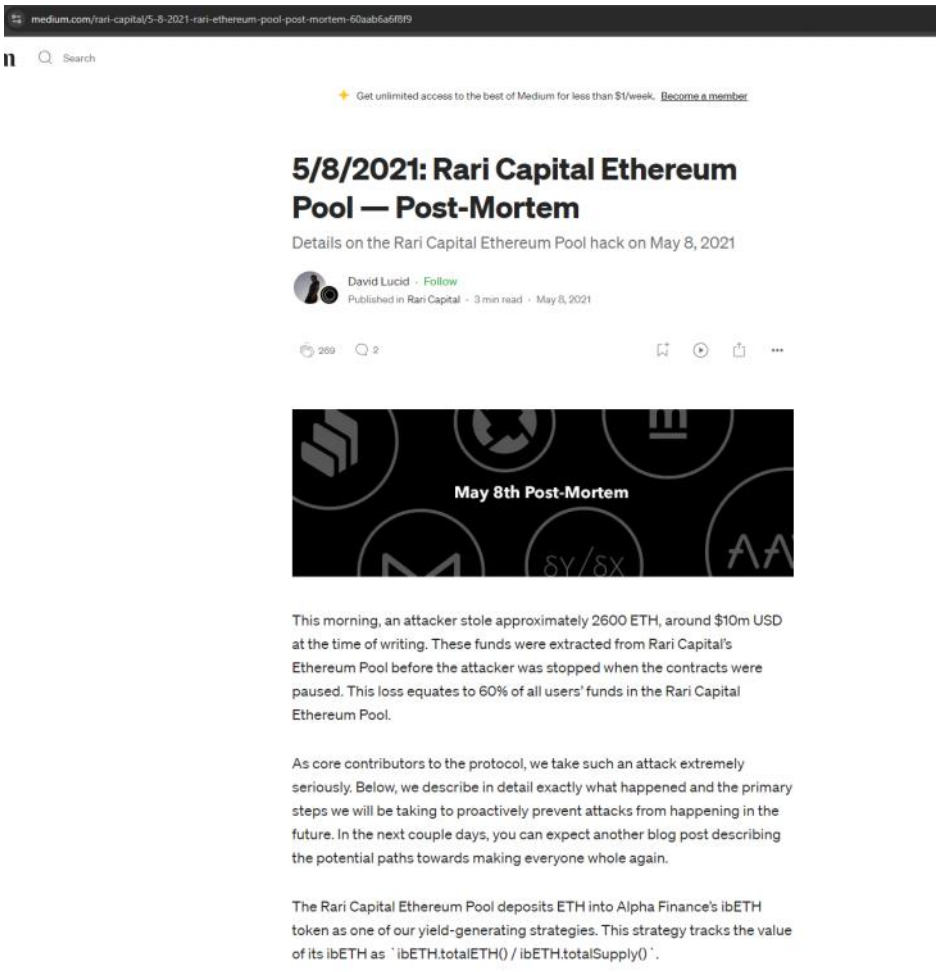


Rari Capital 2021

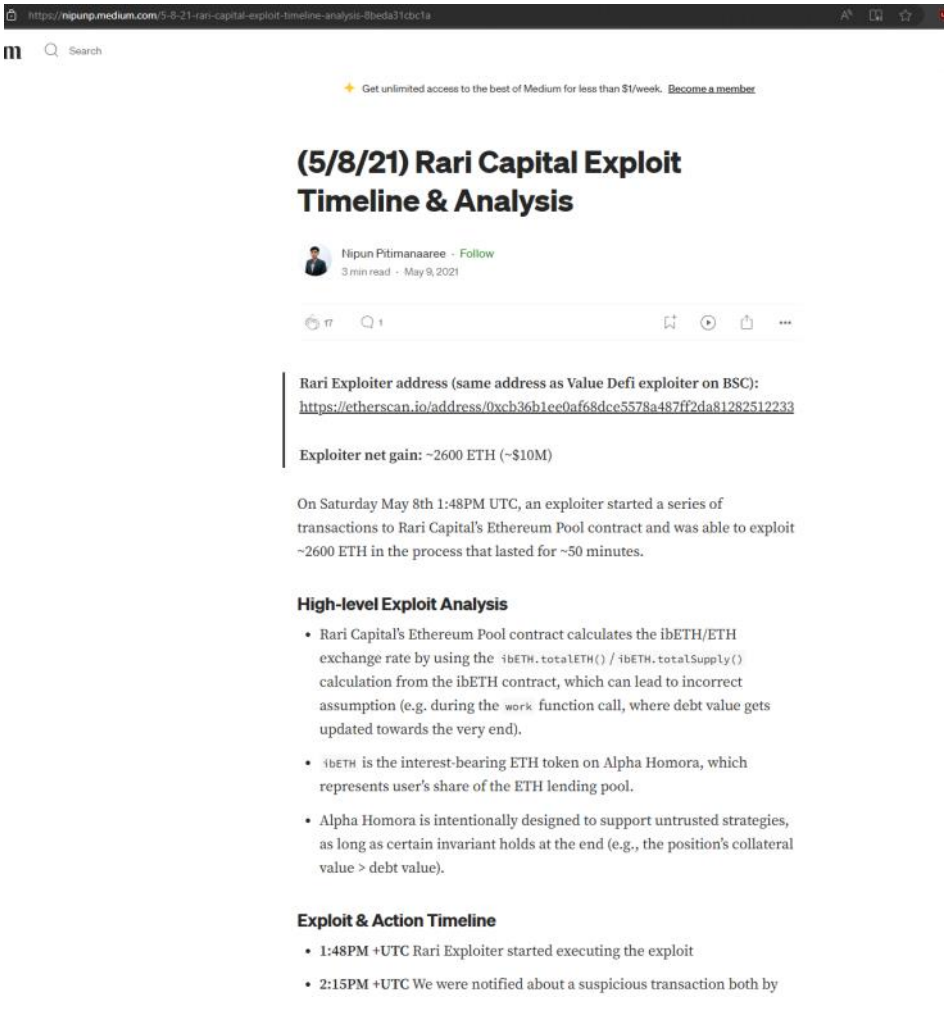
Thursday, September 12, 2024 10:59 AM

On 05/08/2021, David Lucid, a cofounder of Rari Capital, published on Medium.com a post-mortem on an exploit of their protocol. In his blog, he states that the exploit took place in the morning of 05/08/2021 and resulted in the stealing of approximately 2,600 ETH.

Specifically, Lucid explains that the exploit involved Rari Capital's connection with Alpha Finance.



On May 9, 2021, Nipun Pitimanaaree, the lead Engineer at Alpha Finance published a blog providing more detail about the attack on Rari Capital.



https://nipunp.medium.com/5-8-21-rari-capital-exploit-timeline-analysis-8beda31cbc1a

Search

Get unlimited access to the best of Medium for less than $1/week. Become a member

(5/8/21) Rari Capital Exploit Timeline & Analysis

Nipun Pitimanaaree · Follow
3 min read · May 9, 2021

17 1

> **Rari Exploiter address (same address as Value Defi exploiter on BSC):**
> https://etherscan.io/address/0xcb36b1ee0af68dce5578a487ff2da81282512233
>
> **Exploiter net gain:** ~2600 ETH (~$10M)

On Saturday May 8th 1:48PM UTC, an exploiter started a series of transactions to Rari Capital's Ethereum Pool contract and was able to exploit ~2600 ETH in the process that lasted for ~50 minutes.

High-level Exploit Analysis

- Rari Capital's Ethereum Pool contract calculates the ibETH/ETH exchange rate by using the `ibETH.totalETH()` / `ibETH.totalSupply()` calculation from the ibETH contract, which can lead to incorrect assumption (e.g. during the `work` function call, where debt value gets updated towards the very end).
- `ibETH` is the interest-bearing ETH token on Alpha Homora, which represents user's share of the ETH lending pool.
- Alpha Homora is intentionally designed to support untrusted strategies, as long as certain invariant holds at the end (e.g., the position's collateral value > debt value).

Exploit & Action Timeline

- **1:48PM +UTC** Rari Exploiter started executing the exploit
- **2:15PM +UTC** We were notified about a suspicious transaction both by

This blog post specifically mentions the attackers Ethereum address:
0xCB36b1ee0Af68Dce5578a487fF2Da81282512233

An analysis of the transactions associated with this Ethereum address shows that consistent with the blog articles, between 05/08/2021 13:48 UTC and 05/08/2021 14:40 UTC, a sequence of transactions took place netting the attackers address with stolen ETH.

Poloniex

Thursday, September 12, 2024 12:20 PM

In November of 2023, Poloniex announced on their website that they were hacked.

Poloniex > News/Announcements > Latest Announcements

Announcement on Poloniex Hack Incident

Dear Poloniex users,

Regarding the Poloniex hack incident, we hereby promise to each Poloniex user that Poloniex maintains a healthy financial position and will fully reimburse the affected funds.

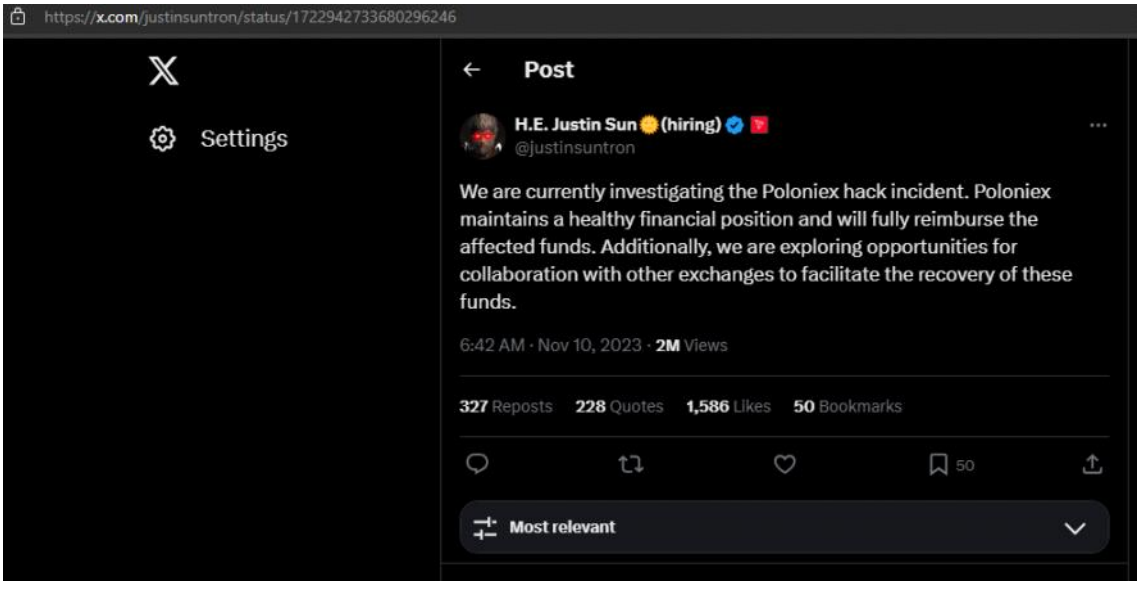
The Poloniex team has successfully identified and frozen a portion of the assets associated with the hacker's addresses to avoid further losses.At present, the losses are within manageable limits, and Poloniex's operating revenue can cover these losses.

Additionally, the team have restored Poloniex's systems, preserved relevant evidence, and in the coming days, we will work diligently to gradually resume deposits and withdrawals on Poloniex, ensuring 100% security. Apologize for any inconvenience this may have caused, thanks for your kind understanding and support!

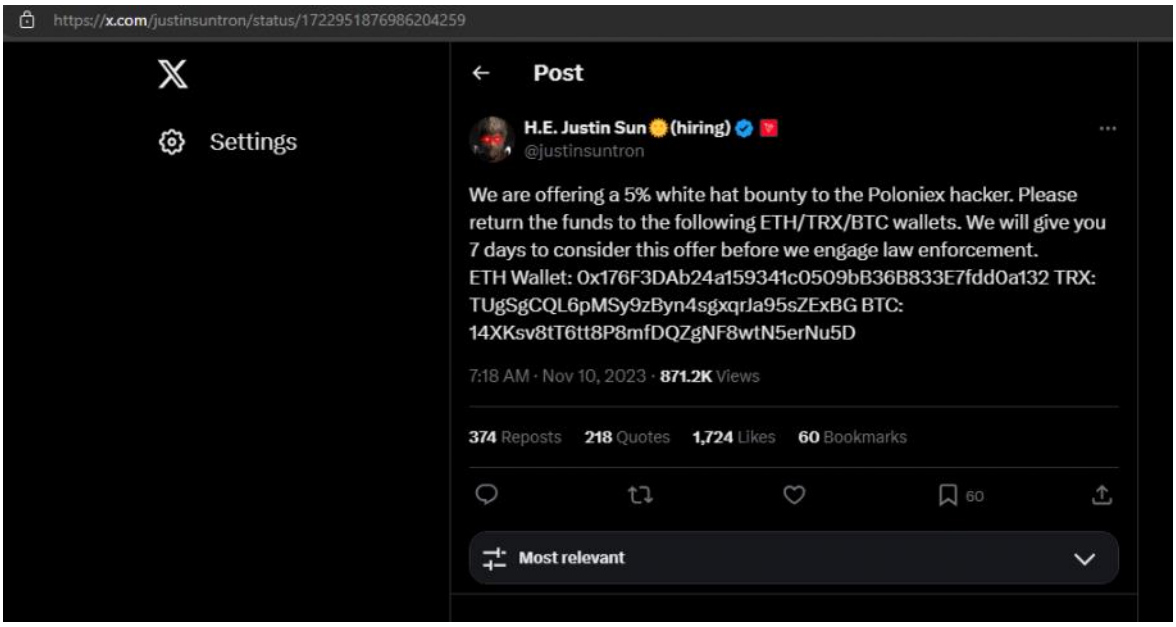
Articles in this section

- Poloniex to Remove 16 Trading Pairs on June 4, 2024
- Poloniex Completes Upgrade of TP/SL Feature for Futures Trading
- Poloniex to Upgrade TP/SL Feature for Futures Trading
- September Giveaway: Enjoy Triple Rewards and Up to 20 USDT for Your Login!
- [PoR] Verification Snapshot Explained
- [PoR] How to Verify My Assets on Poloniex
- Bulk Asset Delistings November 7, 2024

Poloniex investor Justin Sun tweeted on November 10, 2023 that Poloniex suffered a hacking incident and that they were investigating:



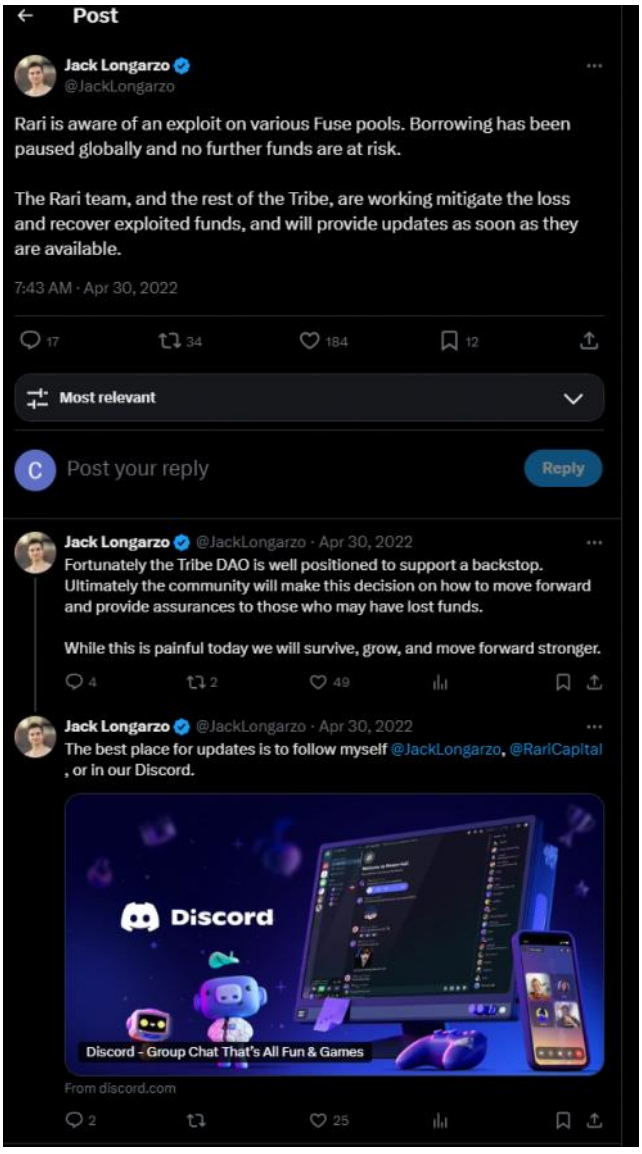
he was offering the Poloniex hacker a 5% white hat bounty.



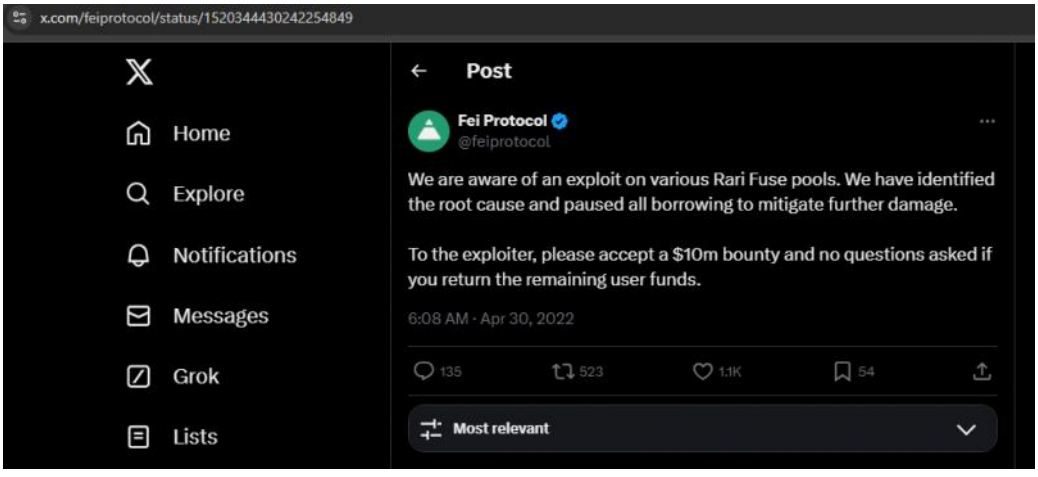
Rari / Fei 2022

Thursday, September 12, 2024 12:48 PM

On 04/30/2022, Jack Longarzo, a developer of Rari Capital, tweeted that Rari Capital was hacked:



The same day, the official Fei Protocol twitter handle posted a $10 million no -questions-asked bounty for the return of funds.



Babylon Finance, a participant in the Rari fuse pool, released a Medium.com blog post describing the Rari attack:

medium.com/babylon-finance/babylon-lending-markets-fuse-fei-exploit-d8daa02c40b9

Containing the Fuse Exploit

Ramon Recuero · Follow
Published in Babylon.finance · 5 min read · May 2, 2022

161

Babylon is a community-led asset management protocol that enables users to create investment clubs (we call them gardens) and invest in DeFi together. It's built on the Ethereum network and it's non-custodial, transparent, permissionless, and governed by the community. BABL is the governance token behind it.

TLDR: Babylon was not hacked. Strategies that deposited into the fuse pool will be backstopped. There is going to be an on-chain proposal in FEI/Rari to refund the loss. If it doesn't go through, Babylon will cover it (up to its means). The goal is that no user funds will be affected.

On February 10th, we released the Babylon Lending & Borrowing markets. The Babylon Gold lender pool on Rari allows Babylonians and garden strategies to **deposit $BABL as collateral and borrow assets from it.**

Since its inception, the activity has been increasing until reaching more than **$8M in collateral and $2M in borrowings.**

On April 20th, Rari Fuse pools were hacked and more than $70M was extracted.

The blog post goes on to reveal that the attacker's Ethereum address is 0x6162759edad730152f0df8115c698a42e666157f:

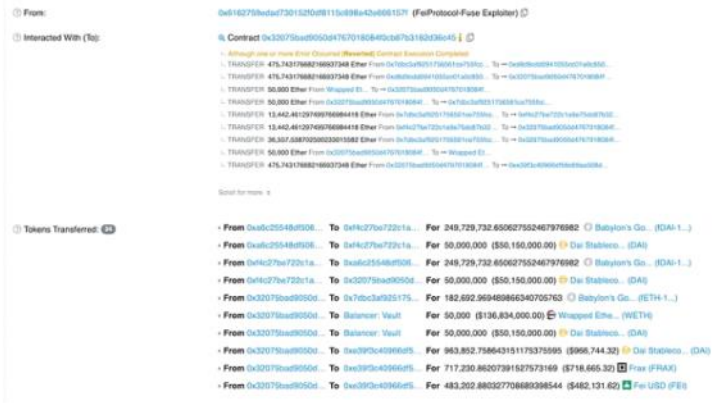
https://medium.com/babylon-finance/babylon-lending-markets-fuse-fei-exploit-d8daa02c40b9

Search

The TVL in our **Fuse Pool jumped from 8.7M to 46.8M** and the borrowings increased from $2.1M to $43.7M 😱

WTH happened? Shortly afterward we start looking at the transactions of our Comptroller markets on Etherscan and here there was:

https://etherscan.io/tx/0x254735c6c14e4d338b1cc5bca43aab6b0f395ae06085013b1b2527180d270a31



The following account 0x6162759edad730152f0df8115c698a42e666157f managed to extract **$3.41M of collateral from our Fuse Pool** between ETH, DAI, FRAX and FEI.

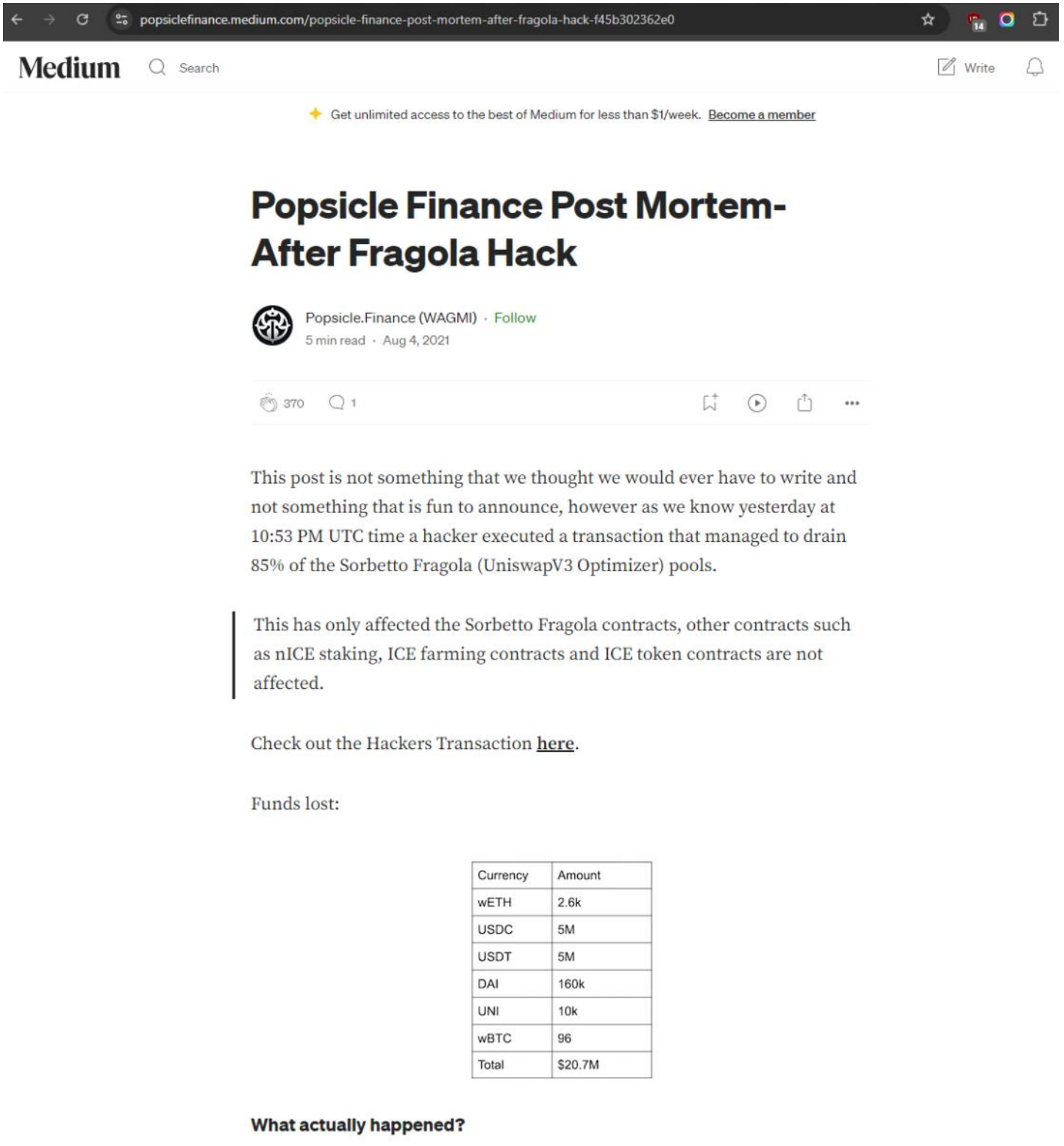
Three Babylon gardens had strategies active on the Fuse Pool: ⛲ The Fountain of ETH, 💲 The Stable Garden, and Stable Pebble. Immediately, we took the following measures:

An analysis of this Ethereum address shows activity consistent with an attack on FeiProtocol:

Popsicle

Friday, September 13, 2024 12:35 PM

On 8/4/2021, Popsicle Finance posted on their official Medium.com blog account that they had been hacked on 08/03/2021.



popsiclefinance.medium.com/popsicle-finance-post-mortem-after-fragola-hack-f45b302362e0

Medium Search Write

Get unlimited access to the best of Medium for less than $1/week. Become a member

Popsicle Finance Post Mortem- After Fragola Hack

Popsicle.Finance (WAGMI) · Follow

5 min read · Aug 4, 2021

370 1

This post is not something that we thought we would ever have to write and not something that is fun to announce, however as we know yesterday at 10:53 PM UTC time a hacker executed a transaction that managed to drain 85% of the Sorbetto Fragola (UniswapV3 Optimizer) pools.

> This has only affected the Sorbetto Fragola contracts, other contracts such as nICE staking, ICE farming contracts and ICE token contracts are not affected.

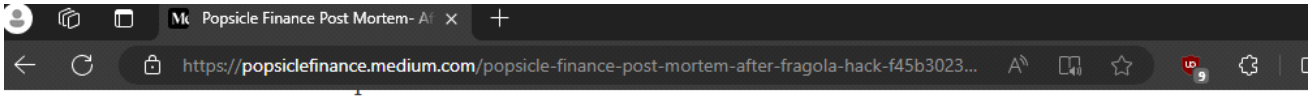
Check out the Hackers Transaction here.

Funds lost:

Currency	Amount
wETH	2.6k
USDC	5M
USDT	5M
DAI	160k
UNI	10k
wBTC	96
Total	$20.7M

What actually happened?

This post stated that the hacker stole tokens, swapped them for Ether, and then cashed out at Tornado Cash:



The hacker made the contract believe that he earned as many fees as the total TVL of the pool and thus is entitled to the $20.7m that was in the pool. This hack was only possible because everything happened within one transaction (due to flashloan).

The hacker took all these captured coins and first swapped them for ETH on Uniswap, and thereafter put them through Tornado.Cash to launder them.

- Swap Transaction 1
- Swap Transaction 2
- Swap Transaction 3
- Swap Transaction 4
- Swap Transaction 5

Sadly, neither we nor our 2 editors (Peckshield & Certik) noticed this bug.

For an in-depth look and analysis of the code, you can refer to this analysis by our friends @blocksecteam in the article here.

So, now what?

First of all, we would like to address the black hat hacker. **Although this may be a long shot we are offering a completely clean $1,000,000 bounty paid in whatever currency he/she likes if funds are returned.**
We are all working here in the new and exciting DeFi space, having people that find vulnerabilities is a part of the ecosystem, however in order to not scare people away we need to make sure they can trust the space. Returning the funds will show the strength of this crypto community.

@danielesesta @squirrelcrypto @popsiclefinance Twitter DMs are open to start the conversation.

The blog post links to the Ethscan transaction which is shows when hovering over the link. The hacker's transaction hash was 0xcd7dae143a4c0223349c16237ce4cd7696b1638d116a72755231ede872ab70fc.

Check out the Hackers Transaction **here**.

Funds lost:

Currency	Amount
wETH	2.6k
USDC	5M
USDT	5M
DAI	160k
UNI	10k
wBTC	96
Total	$20.7M

What actually happened?

You can find the Transaction flow **here**.

In order to start the explanation let's first explain how Fragola actually works.

1. Funds from the user go straight to UniV3.

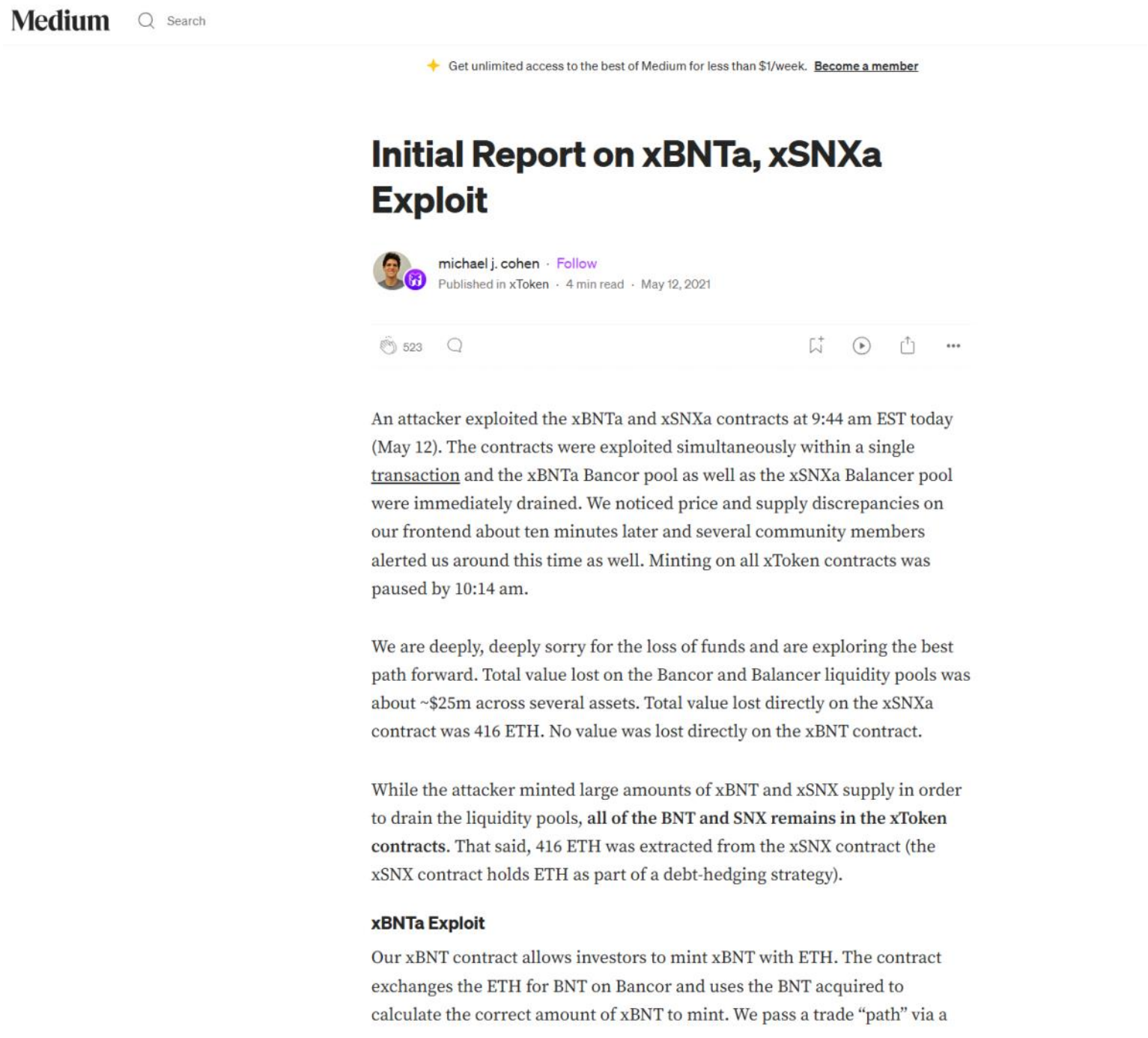
https://etherscan.io/tx/0xcd7dae143a4c0223349c16237ce4cd7696b1638d116a72755231ede872ab70fc

An analysis of this transaction shows that the transaction was ordered by malicious Ethereum address 0xf9E3D08196F76f5078882d98941b71C0884BEa52.

xToken

Tuesday, September 17, 2024 3:34 PM

On May 12, 2021, the founder of xToken posted on xToken's official Medium.com page that they suffered a hack.



Medium Search

Get unlimited access to the best of Medium for less than $1/week. Become a member

Initial Report on xBNTa, xSNXa Exploit

michael j. cohen · Follow
Published in xToken · 4 min read · May 12, 2021

523

An attacker exploited the xBNTa and xSNXa contracts at 9:44 am EST today (May 12). The contracts were exploited simultaneously within a single transaction and the xBNTa Bancor pool as well as the xSNXa Balancer pool were immediately drained. We noticed price and supply discrepancies on our frontend about ten minutes later and several community members alerted us around this time as well. Minting on all xToken contracts was paused by 10:14 am.

We are deeply, deeply sorry for the loss of funds and are exploring the best path forward. Total value lost on the Bancor and Balancer liquidity pools was about ~$25m across several assets. Total value lost directly on the xSNXa contract was 416 ETH. No value was lost directly on the xBNT contract.

While the attacker minted large amounts of xBNT and xSNX supply in order to drain the liquidity pools, **all of the BNT and SNX remains in the xToken contracts**. That said, 416 ETH was extracted from the xSNX contract (the xSNX contract holds ETH as part of a debt-hedging strategy).

xBNTa Exploit

Our xBNT contract allows investors to mint xBNT with ETH. The contract exchanges the ETH for BNT on Bancor and uses the BNT acquired to calculate the correct amount of xBNT to mint. We pass a trade “path” via a

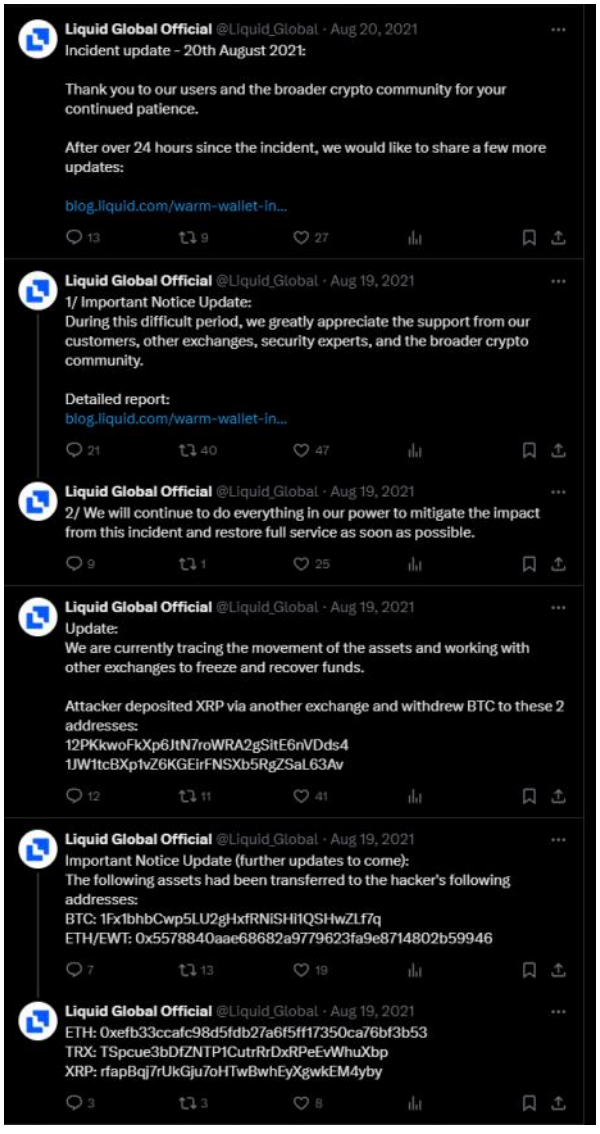
The blog posts mentions that the contracts were stolen in a single transaction. I analyzed that transaction in Etherscan.

Liquid.com

Tuesday, September 17, 2024 4:18 PM

On 08/18/2021, Liquid.com exchange announced on Twitter that they had been hacked:

Liquid.com continued to update its Twitter followers about the hack. On 08/20/2021 they Tweeted a link to a blog post on liquid.com. That blog post no longer exists.



Using archive.org, I recovered a version of this blog post from 08/20/2021. In the post, they explain details of the hack -- approximately $91.35 million of cryptocurrency was stolen comprising 69 different crypto assets.

(disabled for onchain movement) due to the assistance of the crypto community and other exchanges.

- 69 different crypto assets were misappropriated and sent to other exchanges or defi swapping venues.
- Assets placed in Liquid Earn are not impacted.

Liquid's teams are still assessing the attack vector used and taking measures to mitigate the impact to users.

More information will be provided as it becomes available via Liquid Help Center & Liquid Global Twitter.

During this difficult period we greatly appreciate the support from our customers, other exchanges, security experts, and the broader crypto community. Liquid will continue to do everything in its power to mitigate the impact from this incident and restore full service as soon as possible.

These are the list of known addresses used by the un-authorised party:

Currency	Wallet Address
BTC	1Fx1bhbCwp5LU2gHxfRNiSHi1QSHwZLf7q
ETH/ERC-20	0x5578840aae68682a9779623fa9e8714802b59946
ETH	0x8762db106b2c2a0bccb3a80d1ed41273552616e8
ETH	0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53
ETH	0xca0e7269600d353f70b14ad118a49575455c0f2f
TRX	TSpcue3bDfZNTP1CutrRrDxRPeEvWhuXbp
XRP	rfapBqj7rUkGju7oHTwBwhEyXgwkEM4yby

The blog specifies the ETH/ERC20 addresses used to steal funds:

0x5578840aae68682a9779623fa9e8714802b59946
0x8762db106b2c2a0bccb3a80d1ed41273552616e8
0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53
0xca0e7269600d353f70b14ad118a49575455c0f2f

Ether Heist

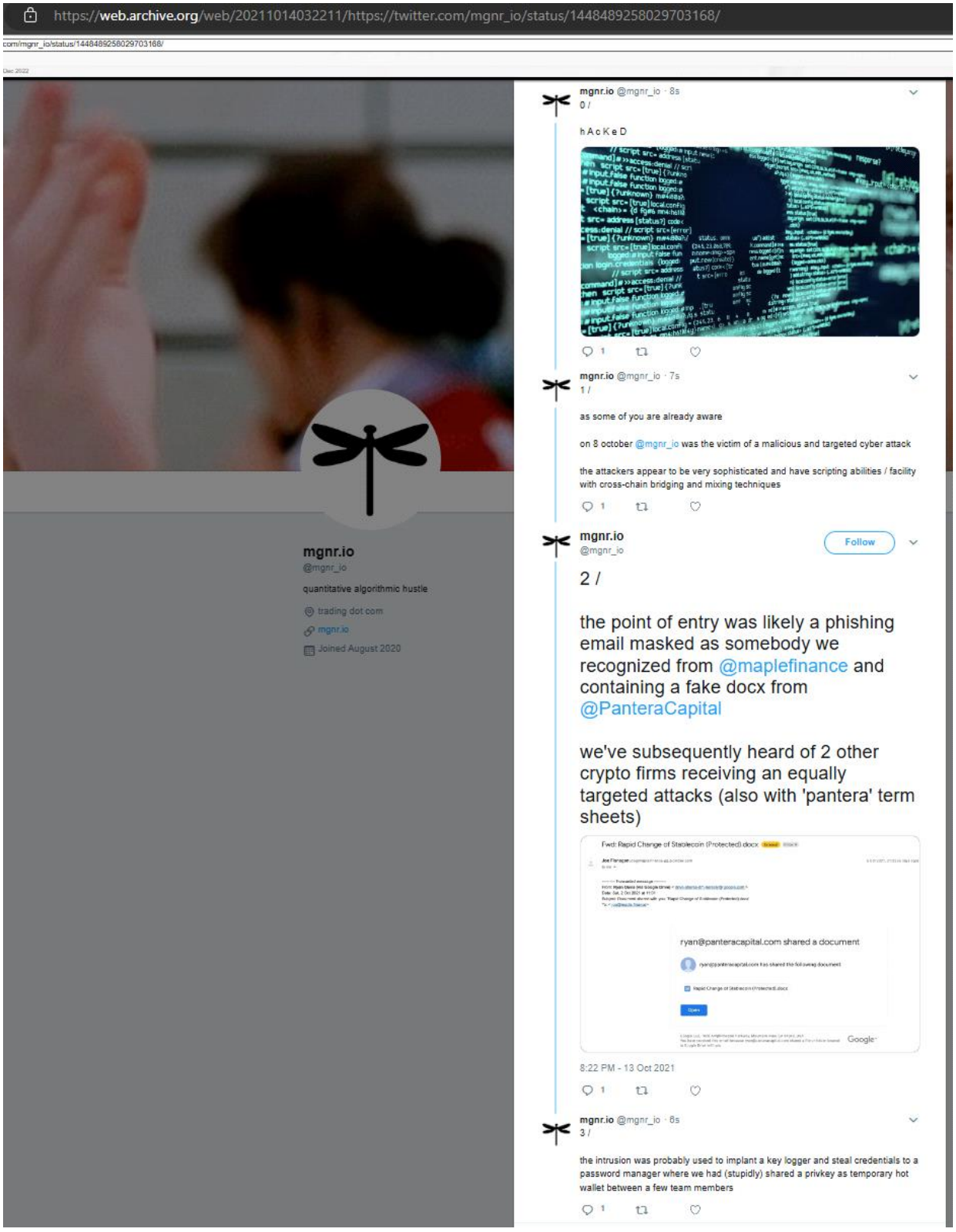
Ethereum address 0xefb33ccafC98d5fDB27A6F5Ff17350CA76BF3b53 received approximately 538 ETH on 08/19/2021 01:14 UTC consistent with the blog post. On 07/18/2022 09:28 UTC, approximately 538 ETH was transferred to address 0xE88243506FCc79052d85ad449eF6A02ACE51c3c6 on 07/18/2022 09:28 UTC.

MGNR.io

Wednesday, September 18, 2024 3:02 PM

On October 13, 2021, the official Twitter account of mgnr.io (@mgnr_io) announced that they had been hacked on October 8, 2021. The tweet has been deleted, but I was able to find a copy of it:

https://web.archive.org/web/20211014032211/https://twitter.com/mgnr_io/status/1448489258029703168/



On October 8, 2021, the mgnr.io team made a complaint with FBI Los Angeles stating that they were hacked and that approximately $35 million worth of cryptocurrency was stolen and sent to Ethereum

bZx

Wednesday, September 18, 2024 4:41 PM

On 11/05/2021, bZx published a "Preliminary Post Mortem" on their official website. The website has been since deleted, but I recovered a copy from archive.org.

Preliminary Post Mortem

We are still investigating, as new information comes to light and unfolds, we will update this post with new information.

Summary

A bZx developer had his personal wallet's private keys taken in a phishing attack. The phishing attack was similar to one that affected another user recently named "mgnr.io".

The ethereum deployment of bZx protocol is safe following the compromise of an individual bZx developer's computer and their private keys. The Ethereum bZx protocol itself wasn't exploited. Since bZx Protocol on ethereum is governed by a DAO, the ethereum implementation was not affected. Ethereum Governance is also unaffected.

This attack granted the hacker access to the content of the bZx Developers wallet, and also the private keys to the BSC and Polygon deployment of bZx Protocol. After gaining control of BSC and Polygon the hacker drained the BSC and Polygon protocol, then upgraded the contract to allow draining of all tokens that the contracts had given unlimited approval.

Who was affected?

- A bZx Developer
- Lenders, borrowers, and farmers with funds on Polygon and BSC, and those who had given unlimited approvals to those contracts. We are gathering data on the specific wallets which were affected by the attack.
- Funds were also removed from the BSC and Polygon implementation of the protocol.

Impact and Funds Stolen:

_Note: We are investigating further to determine the amount of funds that were stolen. We will update the article once the values have been calculated. _

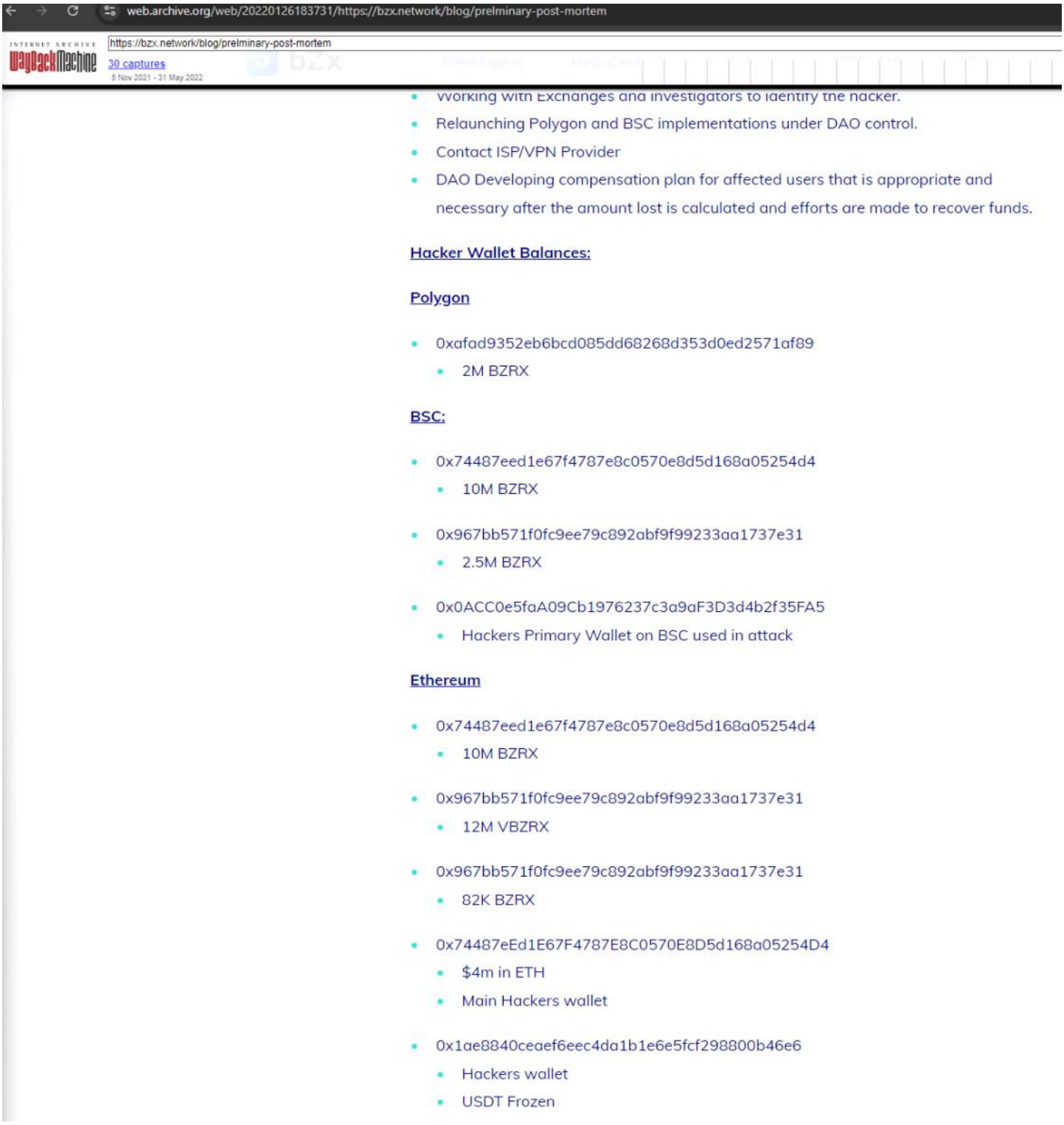
- The hacker stole BZRX on BSC and Polygon using the private key then deposited some of the stolen BZRX funds to be used as collateral to borrow against other funds on the protocol.
- BZRX deployment on Ethereum was not affected and no funds were stolen.
- Funds held in the Polygon and BSC deployment were drained.

The Post Mortem states that bZx developer was hacked and cryptocurrency was stolen starting on 11/05/2021 11:07 UTC. Various tokens on BSC and Polygon were stolen.

The blog post identifies the following Ethereum addresses as belonging to the hacker to include the following:

0x967BB571F0Fc9Ee79c892aBF9f99233AA1737E31
0x0ACC0e5faA09Cb1976237c3a9aF3D3d4b2f35FA5
0x1Ae8840cEaEf6EeC4dA1b1e6e5FCf298800b46e6

0x74487eEd1E67F4787E8C0570E8D5d168a05254D4
0xAfad9352eB6BcD085Dd68268D353d0ed2571aF89



web.archive.org/web/20220126183731/https://bzx.network/blog/prelminary-post-mortem

https://bzx.network/blog/prelminary-post-mortem

30 captures
5 Nov 2021 - 31 May 2022

- Working with Exchanges and Investigators to identify the hacker.
- Relaunching Polygon and BSC implementations under DAO control.
- Contact ISP/VPN Provider
- DAO Developing compensation plan for affected users that is appropriate and necessary after the amount lost is calculated and efforts are made to recover funds.

Hacker Wallet Balances:

Polygon

- 0xafad9352eb6bcd085dd68268d353d0ed2571af89
  - 2M BZRX

BSC:

- 0x74487eed1e67f4787e8c0570e8d5d168a05254d4
  - 10M BZRX
- 0x967bb571f0fc9ee79c892abf9f99233aa1737e31
  - 2.5M BZRX
- 0x0ACC0e5faA09Cb1976237c3a9aF3D3d4b2f35FA5
  - Hackers Primary Wallet on BSC used in attack

Ethereum

- 0x74487eed1e67f4787e8c0570e8d5d168a05254d4
  - 10M BZRX
- 0x967bb571f0fc9ee79c892abf9f99233aa1737e31
  - 12M VBZRX
- 0x967bb571f0fc9ee79c892abf9f99233aa1737e31
  - 82K BZRX
- 0x74487eEd1E67F4787E8C0570E8D5d168a05254D4
  - $4m in ETH
  - Main Hackers wallet
- 0x1ae8840ceaef6eec4da1b1e6e5fcf298800b46e6
  - Hackers wallet
  - USDT Frozen

Consistent with the blog post, an analysis of these five Ethereum addresses shows large token transfers from bZx wallets and subsequent swaps and liquidations to Ether.

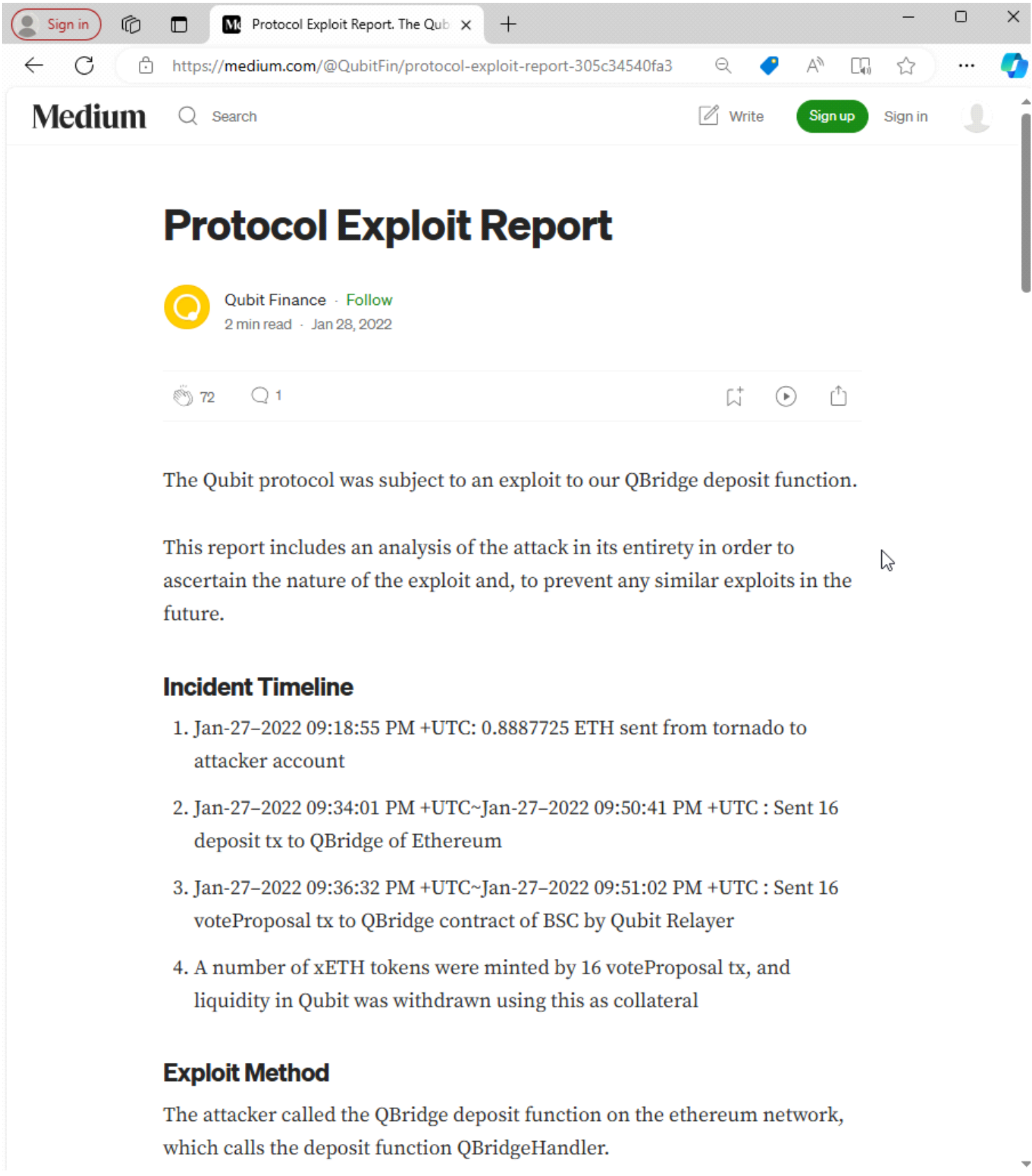
Approximately 9,315 ETH valued at about $39.36 million was sent from these Ethereum addresses to an intermediary Ethereum wallet 0x20d9e73aafe69a3cd66ad7477de7358d0ed44b10 in a series of transactions between 11/15/2021 14:09 UTC and 12/13/2021 05:37 UTC.

An analysis of 0x20d9e73aafe69a3cd66ad7477de7358d0ed44b10 shows that between 11/15/2021 02:14 UTC and 12/13/2021 06:08 UTC, in a series of transactions, approximately 10,960 ETH was transferred to Tornado Cash wallet 0x722122df12d4e14e13ac3b6895a86e84145b6967. The approximate value of this ETH was $45.94 million.

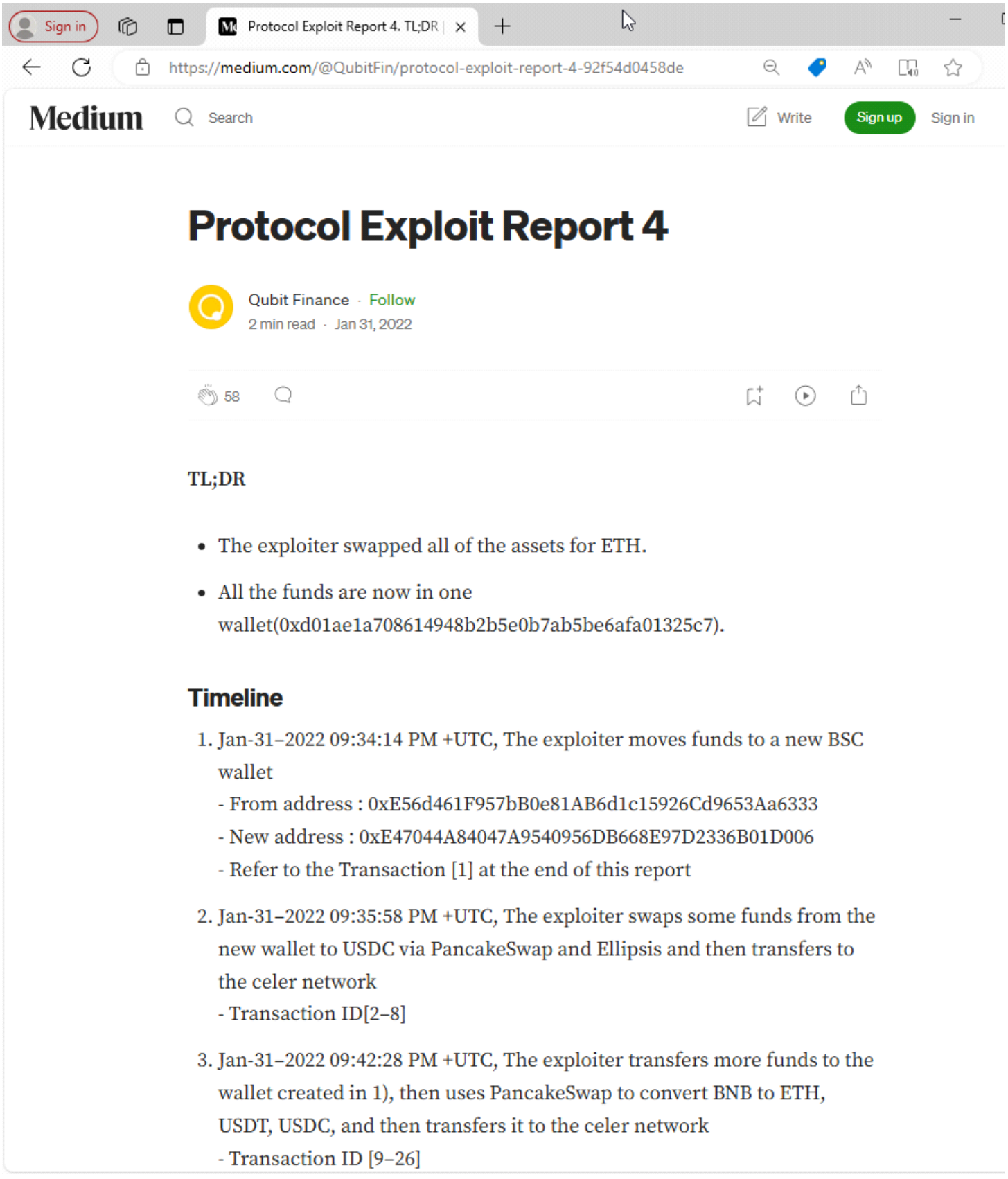
Qubit Finance

Monday, September 23, 2024 1:05 PM

On 01/28/2022, Qubit Finance announced on their official Medium.com blog that their protocol was exploited and funds were stolen. The blog stated that the attack began around 01/27/2022 09:18 UTC:



In the days following the exploit, the Qubit team made additional updates on Medium on the status of the stolen funds. In a blog post dated 01/31/2022, Qubit posts that the exploiter swapped all the stolen assets for Ether and the funds are in wallet 0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7:



An analysis of Ethereum address 0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7, shows that

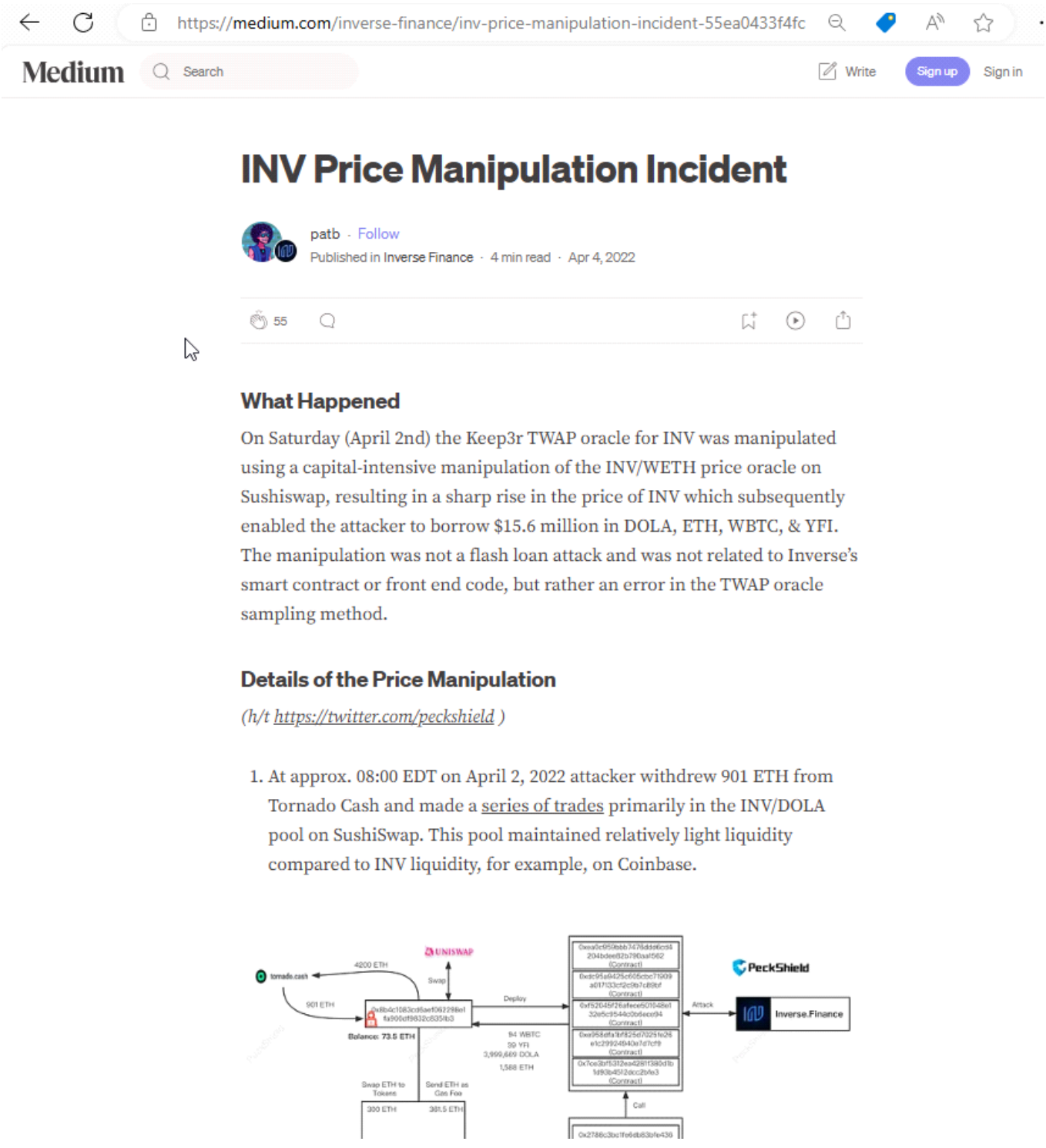
consistent with the blog article, this address received approximately 21,044 ETH valued at $55.07 million between 01/29/2022 15:26 UTC and 01/31/2022 23:39 UTC.

Between 02/07/2022 17:55 UTC and 02/07/2022 18:43 UTC, 7,500 of this ETH valued at approximately $23.56 million was liquidated through Tornado Cash wallet 0x722122df12d4e14e13ac3b6895a86e84145b6967.

Inverse Finance

Monday, September 23, 2024 2:57 PM

On 04/04/2022, a blog post titled "INV Price Manipulation Incident" was posted by the official Inverse Finance account on Medium.com. That article stated that on 04/02/2022, Inverse Finance had approximately $15.6 million in cryptocurrency stolen through a market manipulation exploit.



https://medium.com/inverse-finance/inv-price-manipulation-incident-55ea0433f4fc

Medium Search Write Sign up Sign in

INV Price Manipulation Incident

patb · Follow

Published in Inverse Finance · 4 min read · Apr 4, 2022

55

What Happened

On Saturday (April 2nd) the Keep3r TWAP oracle for INV was manipulated using a capital-intensive manipulation of the INV/WETH price oracle on Sushiswap, resulting in a sharp rise in the price of INV which subsequently enabled the attacker to borrow $15.6 million in DOLA, ETH, WBTC, & YFI. The manipulation was not a flash loan attack and was not related to Inverse's smart contract or front end code, but rather an error in the TWAP oracle sampling method.

Details of the Price Manipulation

(h/t https://twitter.com/peckshield)

1. At approx. 08:00 EDT on April 2, 2022 attacker withdrew 901 ETH from Tornado Cash and made a series of trades primarily in the INV/DOLA pool on SushiSwap. This pool maintained relatively light liquidity compared to INV liquidity, for example, on Coinbase.

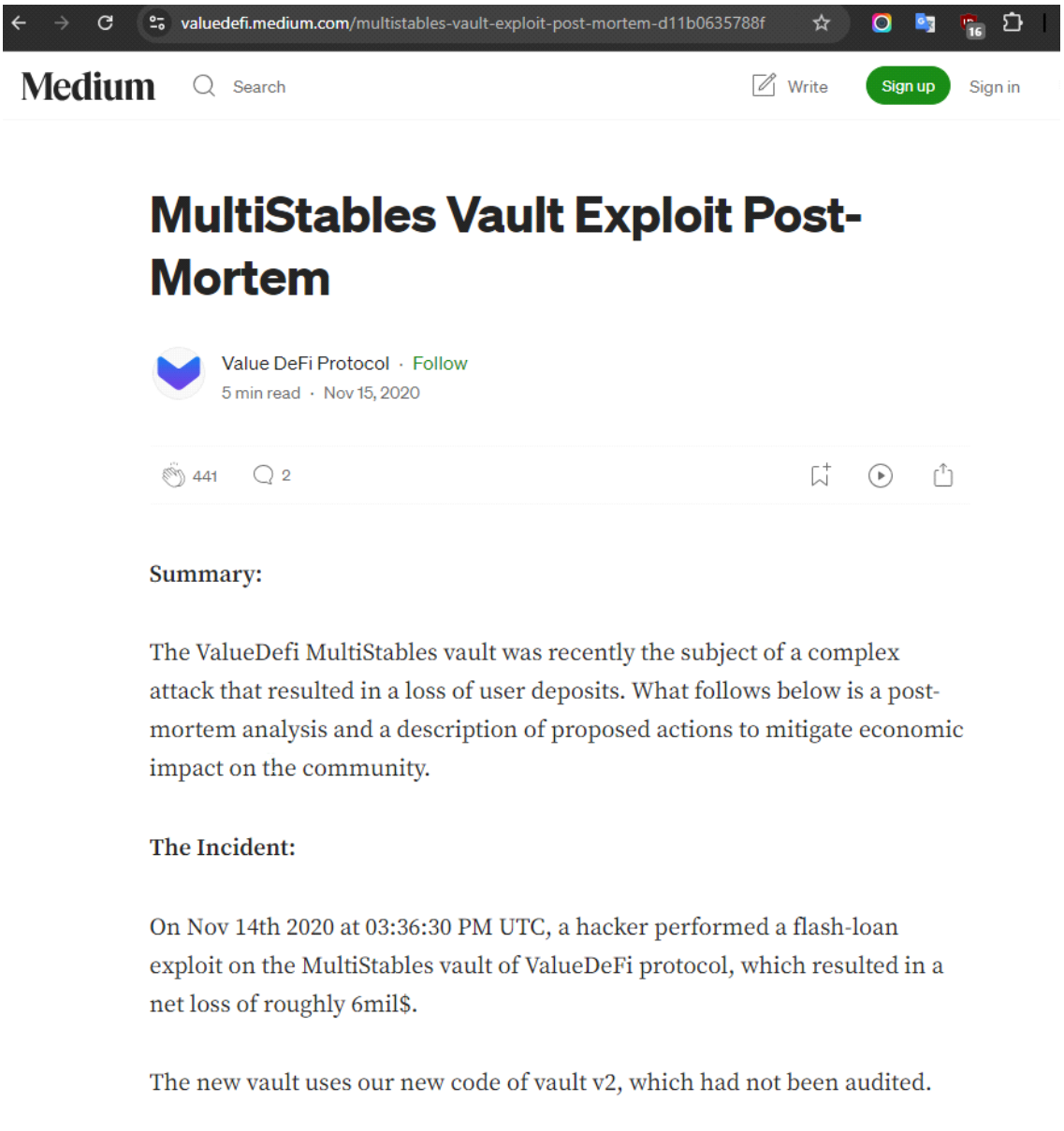
According to the blog post, the stolen funds were transferred to Ethereum address 0x8b4c1083cd6aef062298e1fa900df9832c8351b3.

An analysis of Ethereum address 0x8b4c1083cd6aef062298e1fa900df9832c8351b3 shows that consistent with the blog post, between 04/02/2022 11:04 UTC and 04/02/2022 11:09 UTC the address received 1,588 ETH and a large amount of WBTC, YFI, and DOLA tokens.

ValueDefi

Monday, September 23, 2024 4:47 PM

On 11/15/2020, Value DeFI posted on their official Medium.com blog page that they were exploited by a hacker on 11/14/2020 15:36 UTC resulting in a loss of approximately $6 million.



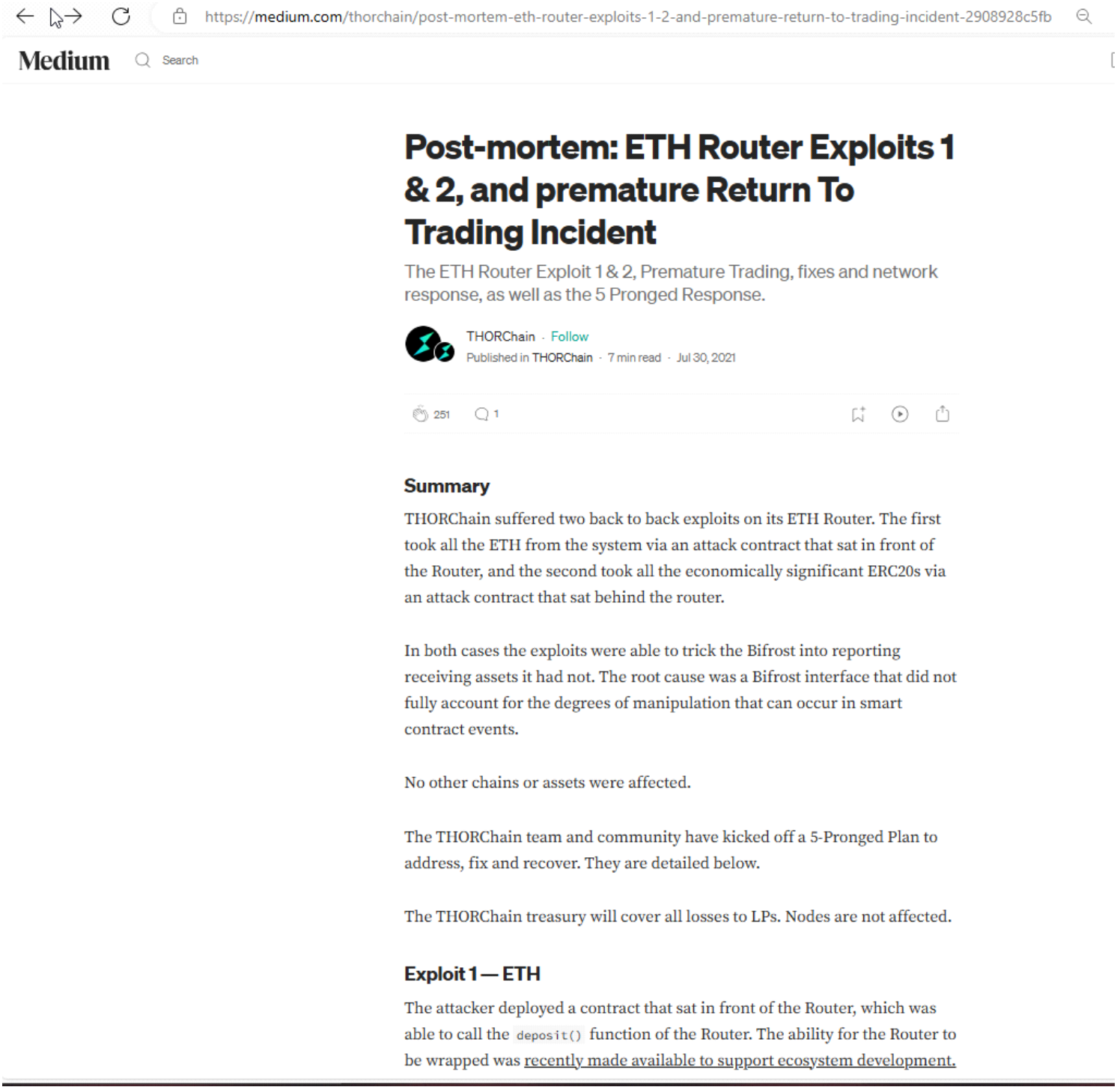
The blog post details the transaction hash of the exploit as 0x46a03488247425f845e444b9c10b52ba3c14927c687d38287c0faddc7471150a. An analysis of this transaction, shows that it is from address 0xa773603b139Ae1c52D05b35796DF3Ee76D8a9A2F.

Thorchain

Monday, September 23, 2024 5:55 PM

On 07/30/2021, the Thorchain official Medium.com account published a blog post titled "Post-mortem: ETH Router Exploits 1 &2, and premature Return to Trading Incident". In the blog post, Thorchain claims they were exploited resulting in a loss of crypto assets.

The article details that the attacker's wallet is 0x8c1944FAC705ef172f21f905b5523Ae260F76d62 .



The write-ups state that the hacker was able to net various ERC-20 tokens to include USDT, XRUNE, and SUSHI resulting in a loss of approximately $8 million.

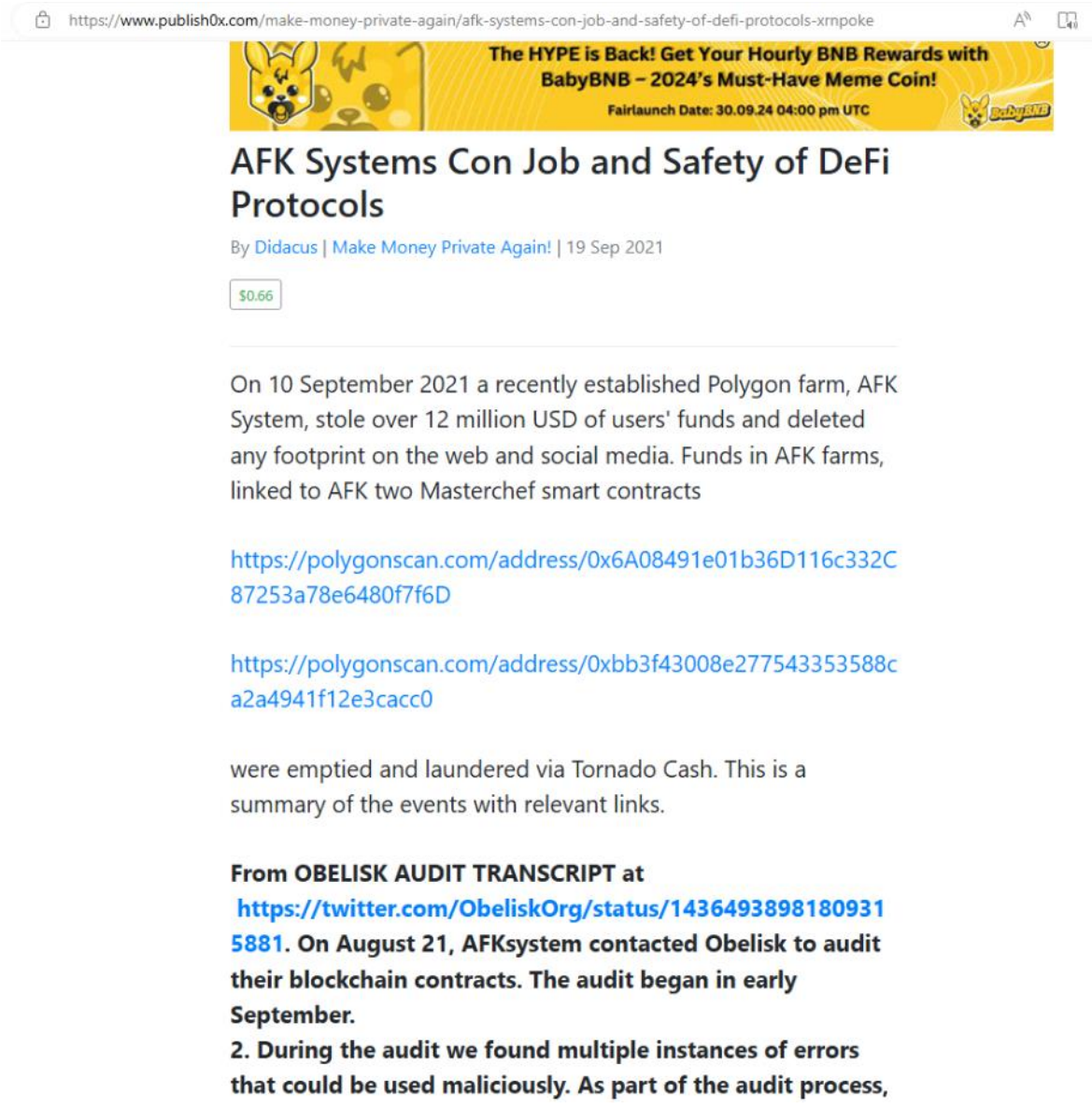
An analysis of the wallet shows that consistent with the post-mortem, various ERC-20 tokens are transferred from Thorswap into the attacker's address between 07/22/2021 19:00 UTC and 21:42 UTC. These tokens were then swapped for approximately 1,934 ETH using SushiSwap and Uniswap on 07/22/2021 22:27 UTC.

AFKFinance

Tuesday, September 24, 2024 9:53 AM

In September 2021, there were reports that AFK Systems conducted a "rug pull" stealing $12 million of its users' funds. The rug pull happened on 09/10/2021.

Here is one blog post detailing the rug pull:



https://www.publish0x.com/make-money-private-again/afk-systems-con-job-and-safety-of-defi-protocols-xrnpoke

AFK Systems Con Job and Safety of DeFi Protocols

By Didacus | Make Money Private Again! | 19 Sep 2021

$0.66

On 10 September 2021 a recently established Polygon farm, AFK System, stole over 12 million USD of users' funds and deleted any footprint on the web and social media. Funds in AFK farms, linked to AFK two Masterchef smart contracts

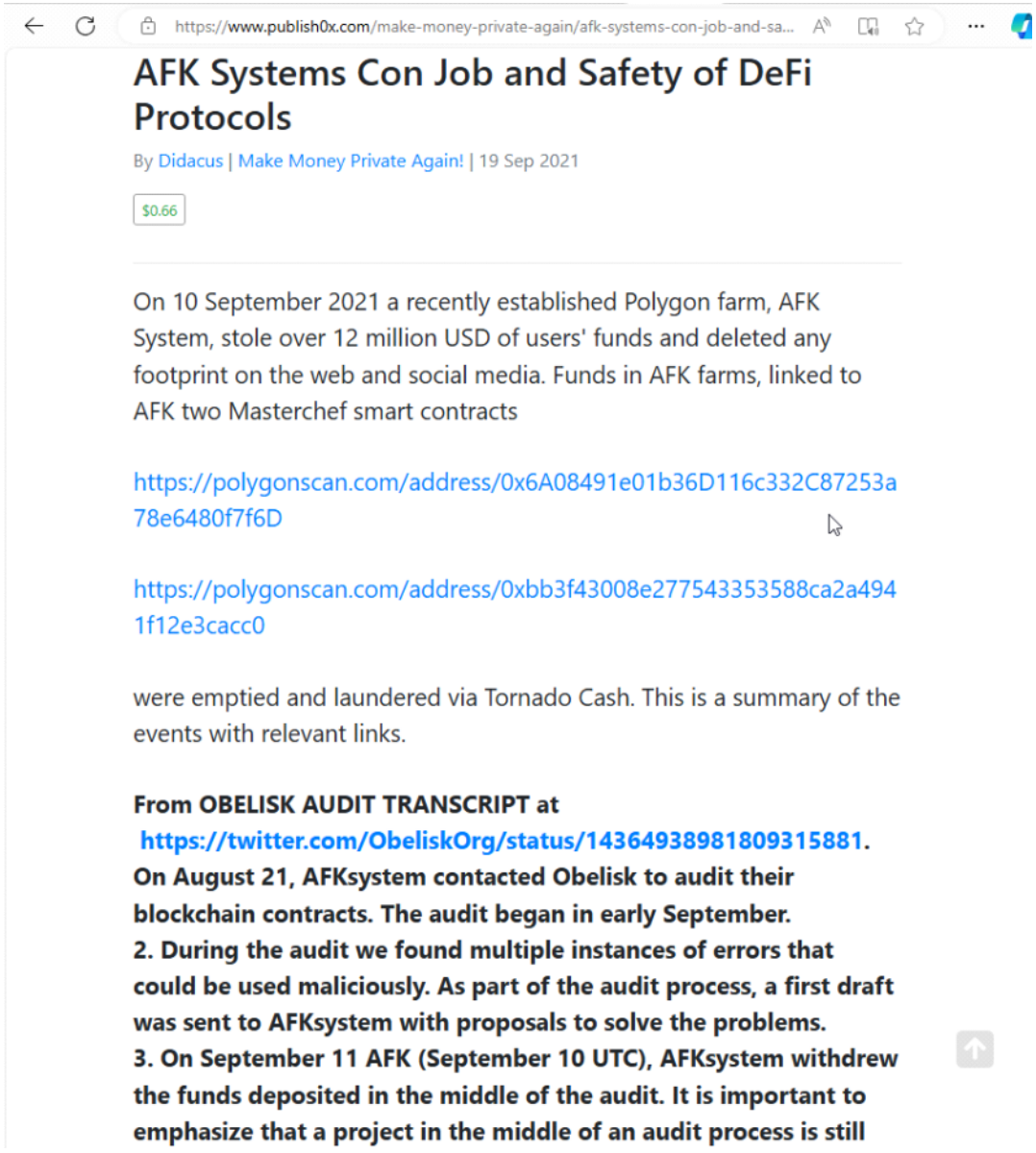
https://polygonscan.com/address/0x6A08491e01b36D116c332C87253a78e6480f7f6D

https://polygonscan.com/address/0xbb3f43008e277543353588ca2a4941f12e3cacc0

were emptied and laundered via Tornado Cash. This is a summary of the events with relevant links.

From OBELISK AUDIT TRANSCRIPT at https://twitter.com/ObeliskOrg/status/1436493898180935881. On August 21, AFKsystem contacted Obelisk to audit their blockchain contracts. The audit began in early September.
2. During the audit we found multiple instances of errors that could be used maliciously. As part of the audit process,

The same author of the blog post wrote a template police report for victims.



https://www.publish0x.com/make-money-private-again/afk-systems-con-job-and-sa...

AFK Systems Con Job and Safety of DeFi Protocols

By Didacus | Make Money Private Again! | 19 Sep 2021

$0.66

On 10 September 2021 a recently established Polygon farm, AFK System, stole over 12 million USD of users' funds and deleted any footprint on the web and social media. Funds in AFK farms, linked to AFK two Masterchef smart contracts

https://polygonscan.com/address/0x6A08491e01b36D116c332C87253a78e6480f7f6D

https://polygonscan.com/address/0xbb3f43008e277543353588ca2a4941f12e3cacc0

were emptied and laundered via Tornado Cash. This is a summary of the events with relevant links.

From OBELISK AUDIT TRANSCRIPT at https://twitter.com/ObeliskOrg/status/1436493898180931588 1. On August 21, AFKsystem contacted Obelisk to audit their blockchain contracts. The audit began in early September. 2. During the audit we found multiple instances of errors that could be used maliciously. As part of the audit process, a first draft was sent to AFKsystem with proposals to solve the problems. 3. On September 11 AFK (September 10 UTC), AFKsystem withdrew the funds deposited in the middle of the audit. It is important to emphasize that a project in the middle of an audit process is still

According to this author, the stolen funds were deposited into Ether address 0x56eb4a5f64fa21e13548b95109f42fa08a644628.

Similarly, an online post by the Quadriga Initiative, a self-described "community-based, not-for-profit crypto watchdog & fraud recovery platform" details the mechanics of the AFK system fraud:

https://quadrigainitiative.com/casestudy/afkfinancegoesafk.php

DESCRIPTION OF EVENTS

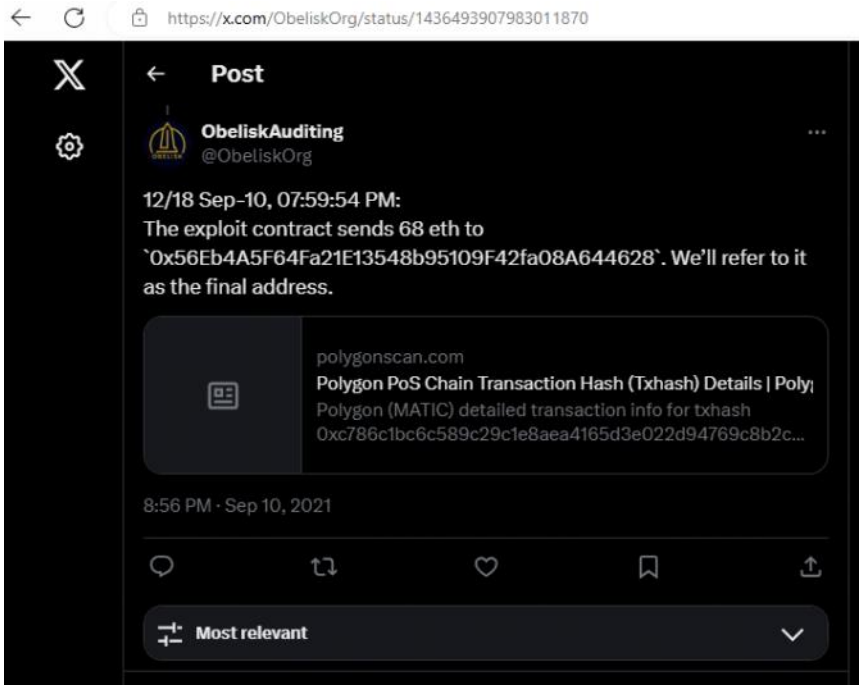
"AFKsystem.Finance is a Decentralized Yield Farming Ecosystem created by Yield Farmers, for Yield Farmers. Our $SILVER token ensures that AFKsystem.Finance is owned by its users. $SILVER will only be rewarded to users who benefit the protocol, thus there will be no single asset farming pools, only single asset Missions (AAVE Vaults)." "[T]the address used in the [contract] was filled using tornado[cash]" on July 8th.

"AFKsystem.Finance launching in less than 24 hours, Polygon newest DeFi Yield Vaults! Partnered with Dfyn exchange, join us at our launch on 19th Aug UTC 2PM! Fairly Launched!"

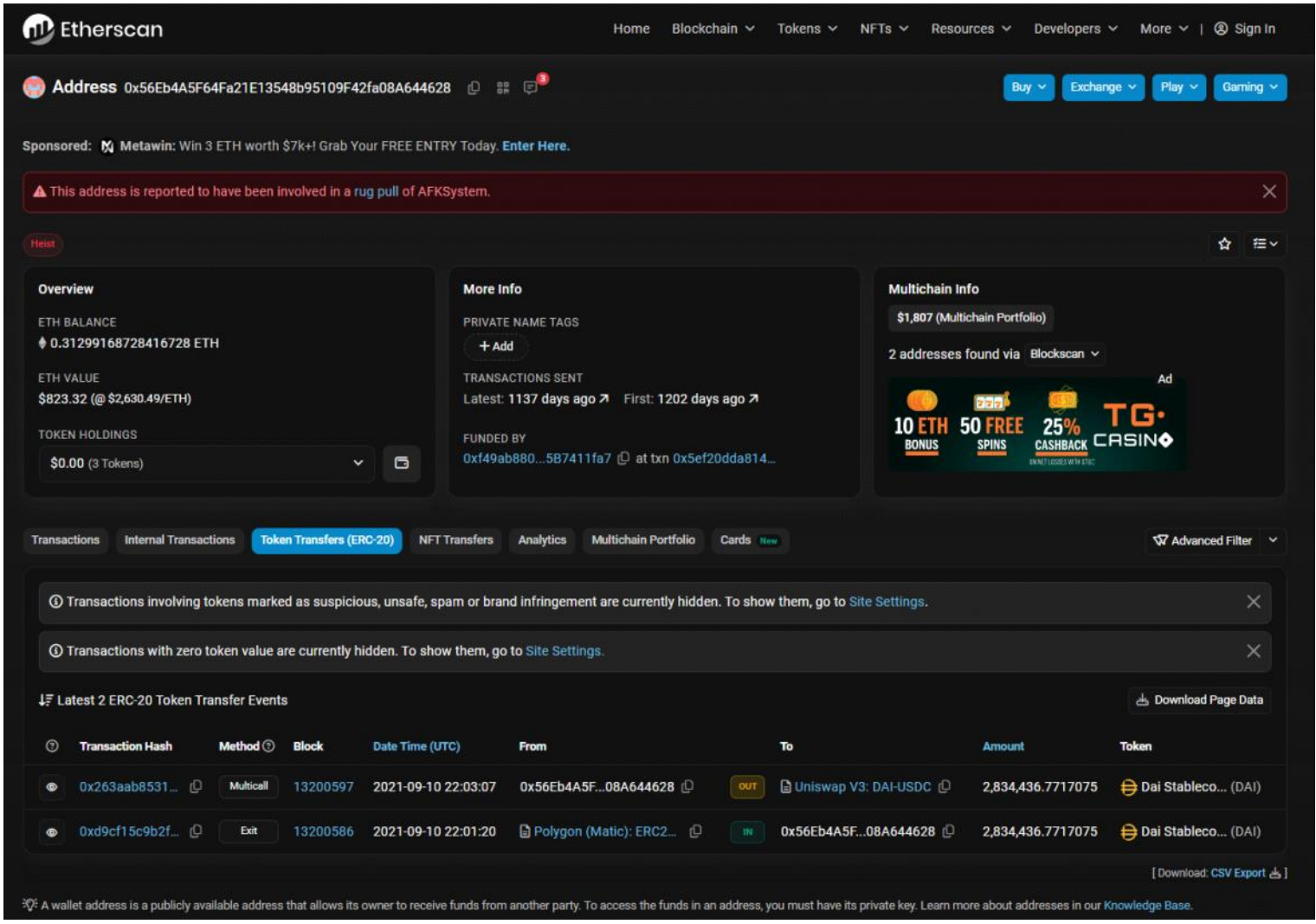
"Our official auditing partner, @0xPaladinSec, has funnily always pointed out these governance privileges to change the router as either high severity or medium severity." "AFK Systems cancelled their Paladin audit in favor of another auditor."

"On the 21st of August, AFK contacted Obelisk for an audit of their smart contracts. The actual audit started at the beginning of September."

ObeliskAuditing, who claims to be the independent auditor of AFKsystem also published a post-mortem in a Twitter thread. They traced the stolen funds and also reported the recipient address as 0x56eb4a5f64fa21e13548b95109f42fa08a644628.



An analysis of the Ethereum address 0x56eb4a5f64fa21e13548b95109f42fa08a644628 shows that consistent with the public reporting, on 09/10/2021 22:01 UTC approximately 2,834,436 DAI tokens are deposited into the address from the Polygon Matic Bridge.



On 09/10/2021 22:03 UTC, the total balance of DAI is swapped for approximately 879 ETH using Uniswap.

DAO Maker

Tuesday, September 24, 2024 11:18 AM

On 08/12/2021, DAO Maker published a blog post on its official Medium.com page titled "DAO Maker Statement". In the blog they announced that their protocol was hacked resulting in a $7 million loss.

DAO Maker Statement — Thursday, 12th of August

B. M. Follow
Aug 12 · 2 min read

The rapid expansion of the DAO Maker has posed several challenges to the ecosystem. These include turbulence in project onboarding and changes to company structure.

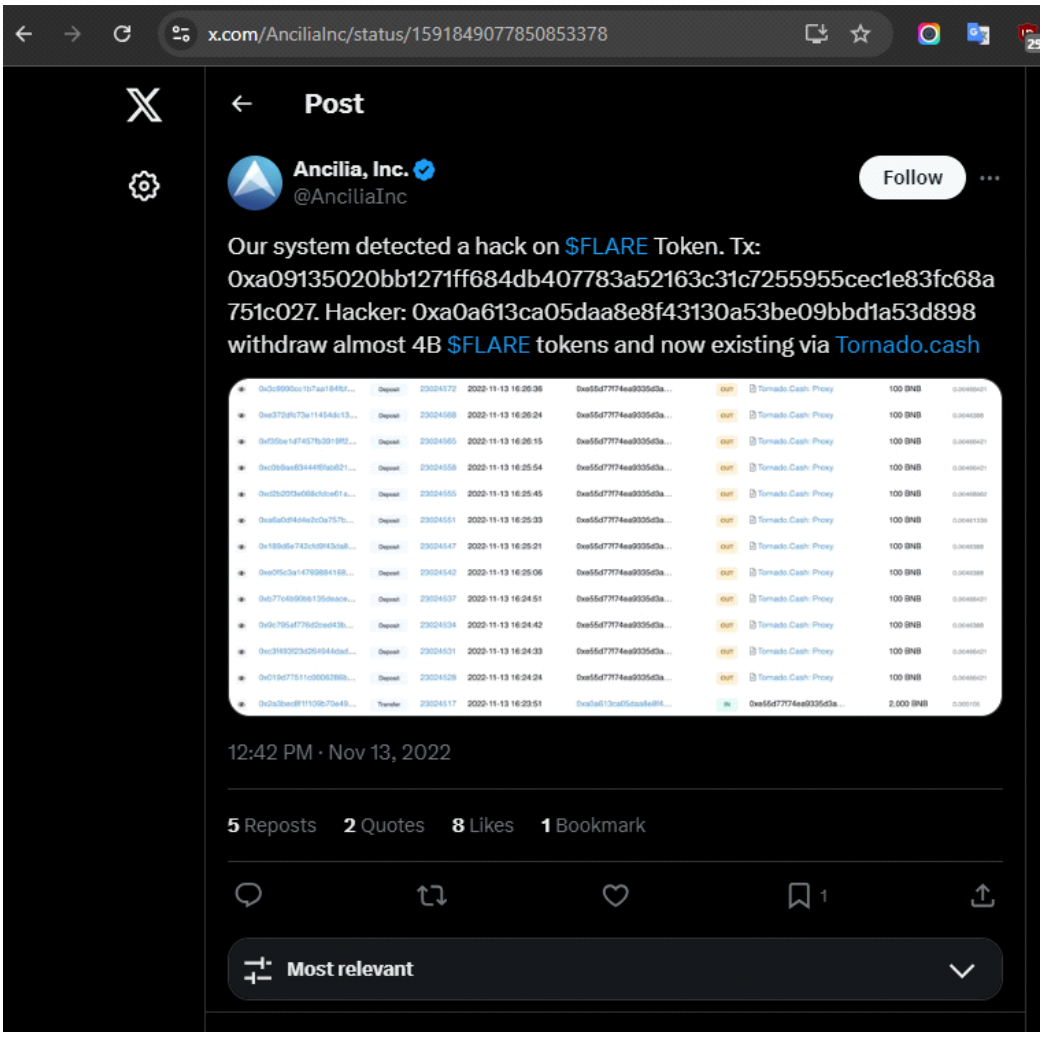
Regretfully, we must announce that in the early hours of August 12th (approx. 1 AM UTC) DAO Maker faced malicious use of one of our wallets with access to admin privileges.

The cybercriminal, after tentatively testing this exploit and managing to

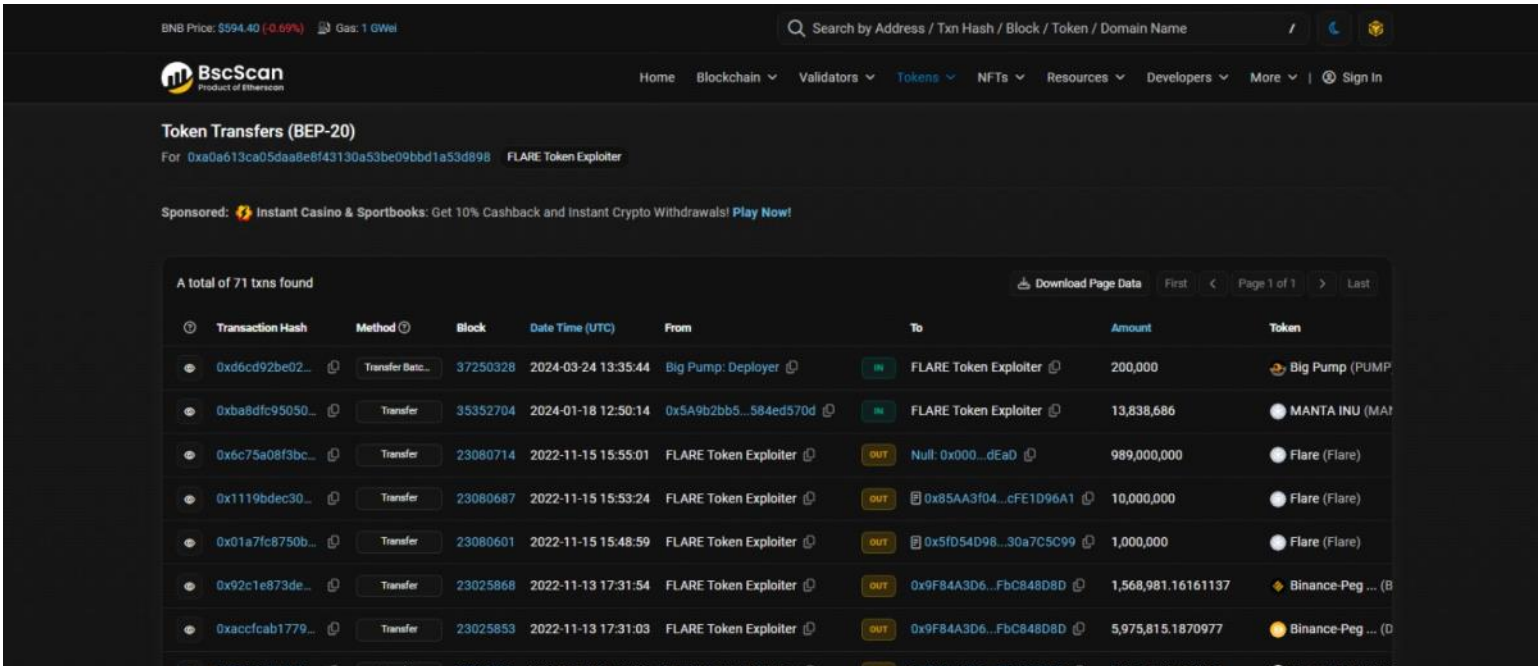
Flare Token

Tuesday, September 24, 2024 11:52 AM

On 11/13/2022 blockchain auditing company Ancilia, Inc. tweeted that they detected a hack on Flare Token. They identified the attacker's address as 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898.



An analysis of that address on the Binance Smart Chain shows that on 11/13/2022 15:29 UTC, consistent with the Tweet, the address 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898 received about 3,973,277,600 Flare tokens in txid 0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027.



Squid Game Token

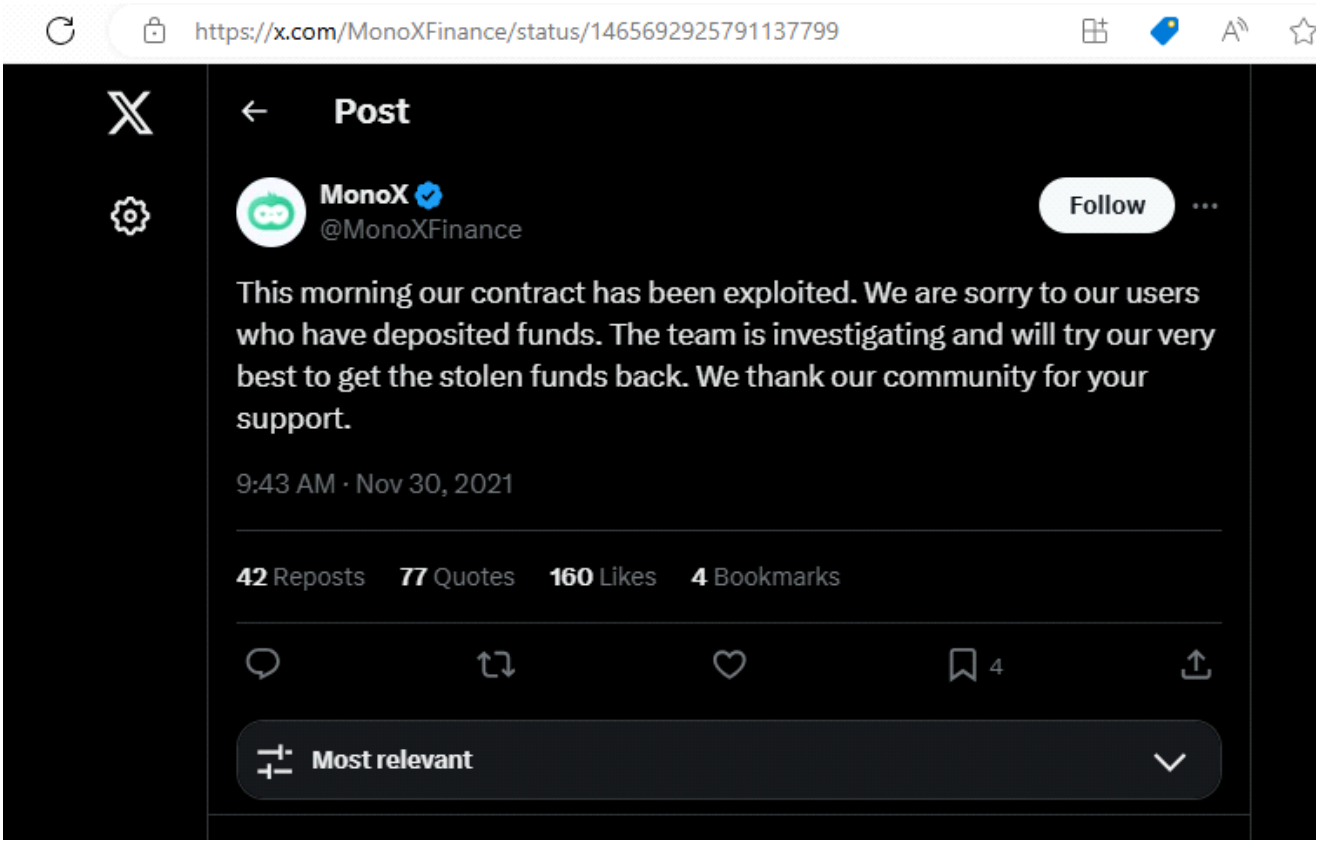
Tuesday, September 24, 2024 12:17 PM

On 11/11/2021, blockchain auditing firm sharkteam.org published a report titled "Squid game Rug pull: Fund flow analysis". In their report they describe a "rug pull" situation where the Squid game coin developers stole investor money.

MonoX Protocol

Tuesday, September 24, 2024 12:31 PM

On 11/30/2021, MonoX tweeted from their official account that their protocol was victimized and funds were stolen:



On 12/01/2021, MonoX published a blog on their official Medium.com account titled "Exploit:Post Mortem". The blog states that approximately $31 million in cryptocurrency was stolen.

https://medium.com/monoswap/exploit-post-mortem-33921a779b43

Medium Search Write Sign up

Exploit: Post Mortem

MonoX Team · Follow
Published in MonoX · 4 min read · Dec 1, 2021

370 4

MONO Family. It's with a heavy heart that we are writing such an update.

The past 24 hours have been difficult, and we're simply at a loss for words. No apologies and no amount of words can describe how the team has been feeling since the attack transpired. We started building over a year ago with a mission to make DeFi more accessible to users and projects. We appreciate all the support we have received along the way from friends, partners, investors and our community of users.

Days like yesterday are horrible, there is no sugar coating the harsh reality of a contract being exploited and people losing money. Our supporters put their faith in a new project like us, and yesterday we let them down.

Security has always been very important to us. We conducted a three-month testnet + bug bounty, and conducted 3 audits prior to launch. In these audits,

This blog links to other published reports analyzing the mechanics of the hack. One such report is published by Rekt.news:

https://rekt.news/monox-rekt/

rekt

T&C | Videos | leaderboard | dark | en

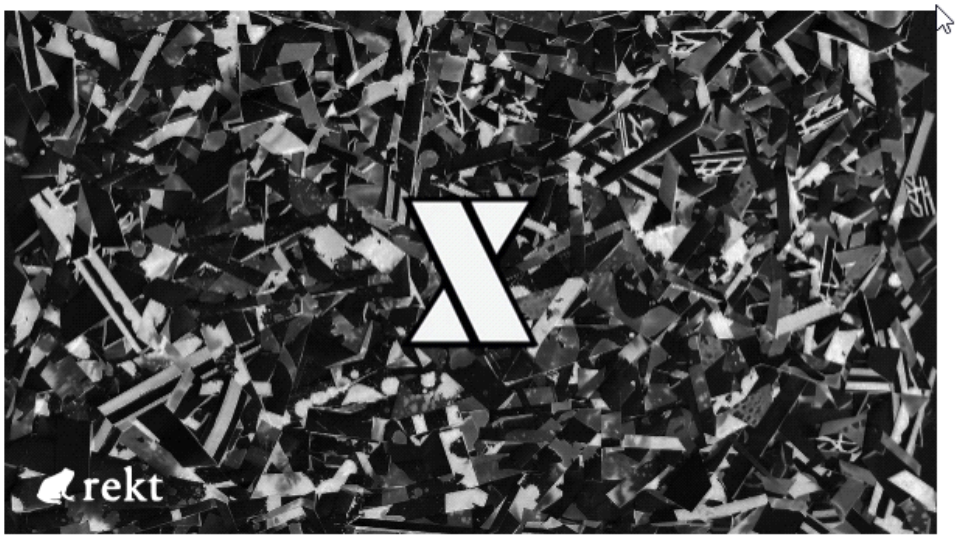
MONOX - REKT

Tuesday, November 30, 2021

MonoX - REKT

read this article also in:

en - es - fr - ko - ru - tr - zh



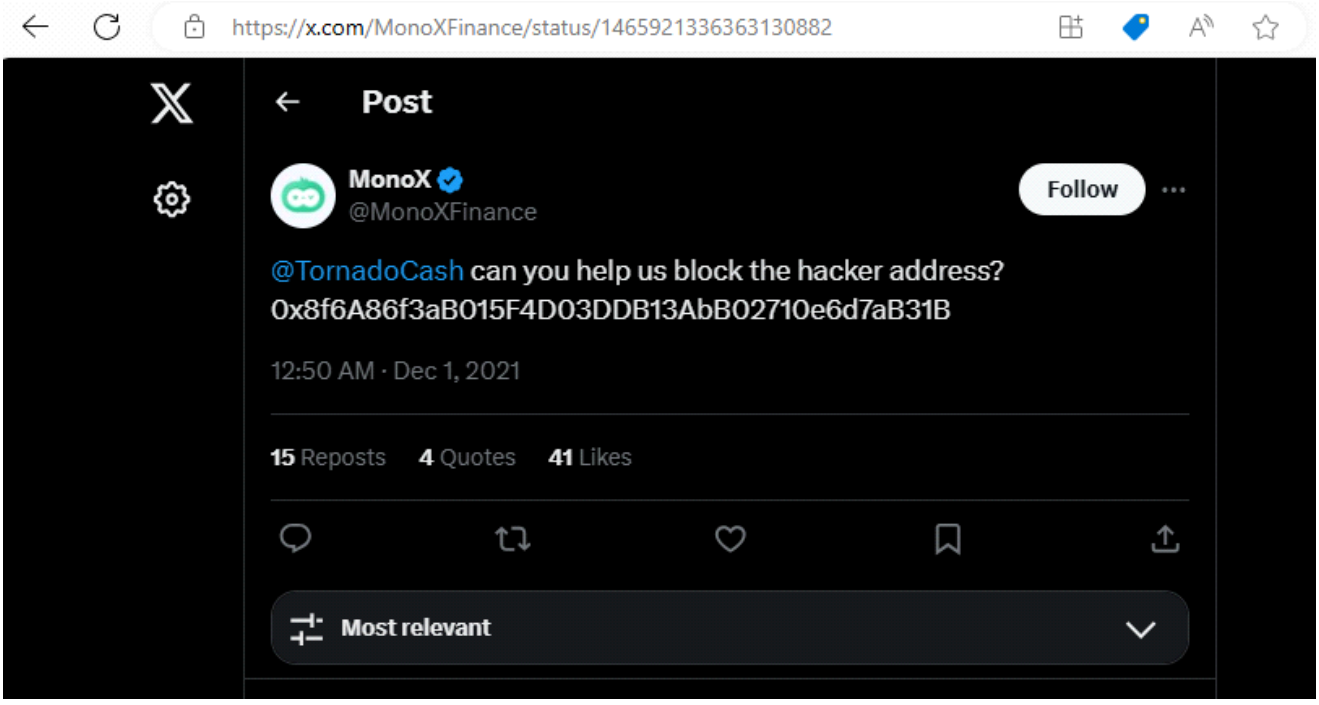
rekt by their own token.

Over $31 million stolen, across two chains, via a price manipulation of the project's native token, MONO.

MonoX, which launched last month on Polygon and Ethereum, is a DEX based on Single Token Liquidity pools. Rather than the standard pool model of paired assets de-

The rekt report states that the stolen funds ultimately were transferred to Ethereum address 0x8f6A86f3aB015F4D03DDB13AbB02710e6d7aB31B.

This attacker address is corroborated by MonoX's official Twitter account in this tweet:



An analysis of this address shows that consistent with the Rekt report, on 11/30/2021 13:27 UTC the address received various ERC-20 tokens valued at $11.89 million to include Wrapped Ether. On 12/01/2021 05:37 UTC, 100 Wrapped Ether is exchanged for 100 ETH deposited into this address. On 12/01/2021 05:44 UTC, 100 ETH valued at approximately $.46 million is transferred to Tornado Cash address 0x722122df12d4e14e13ac3b6895a86e84145b6967.

Similarly, on 02/04/2022 13:21 UTC, 2,149 of Wrapped Ether is exchanged for 2,149 ETH deposited into this address. Between 02/04/2022 13:32 UTC and 02/20/2022 10:00 UTC, through a series of transactions, 2,100 ETH valued at approximately $5.77 million is transferred to Tornado Cash address 0x722122df12d4e14e13ac3b6895a86e84145b6967.

LCX

Tuesday, September 24, 2024 1:52 PM

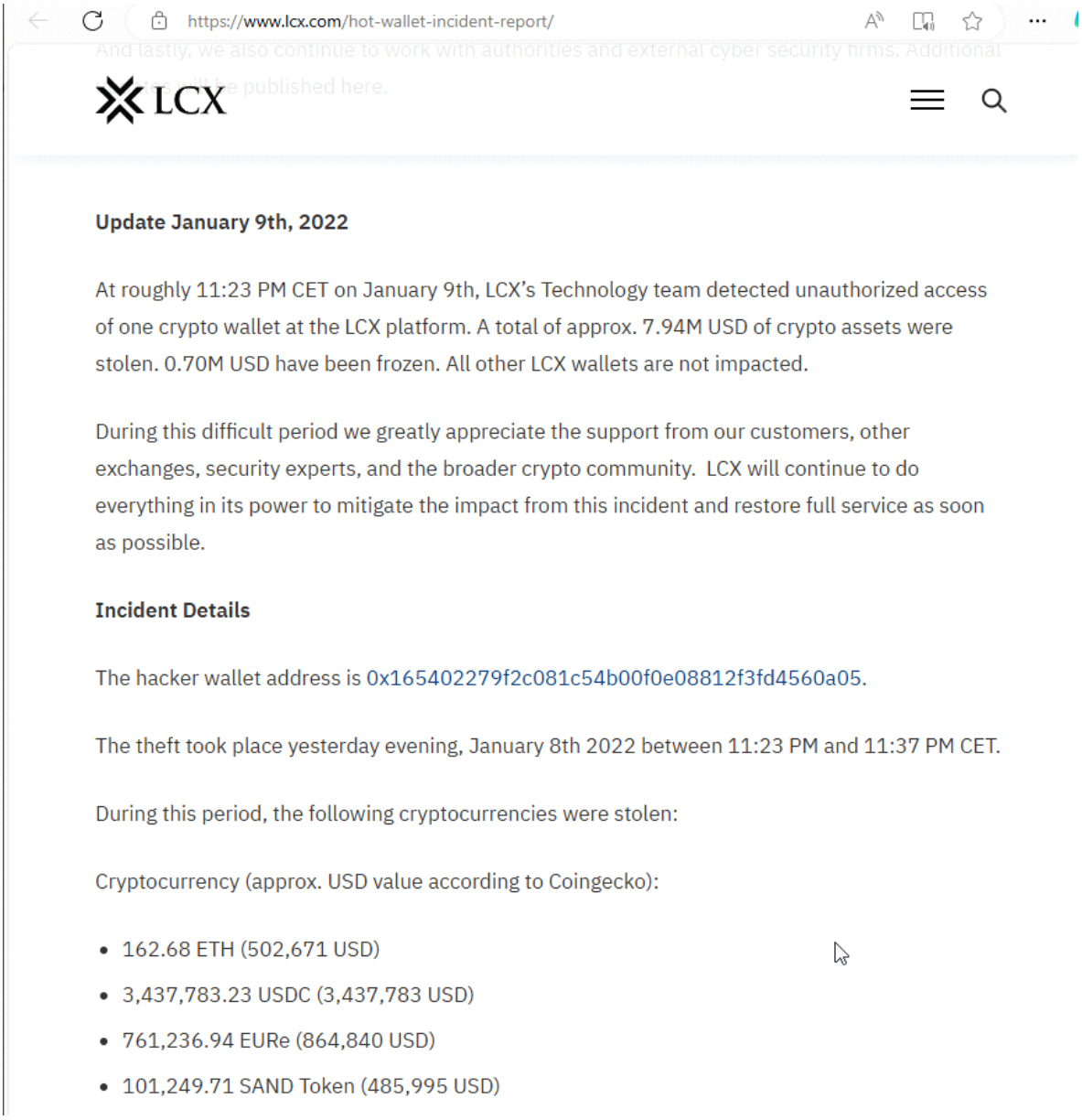
On 01/09/2022, cryptocurrency exchange LCX announced on their website that they suffered a hack on 01/08/2022 that resulted in a loss of approximately $8 million.

Final Update
January 28th 2022

We are happy to announce that all deposit and withdrawal services have resumed 100% operations. Also services in collaboration with Monerium have resumed.

We would like to once again thank our clients, customers, partners, and the broader crypto community for your support during this period.

In this report they detail that the address that received the stolen funds was: 0x165402279f2c081c54b00f0e08812f3fd4560a05.



https://www.lcx.com/hot-wallet-incident-report/

And lastly, we also continue to work with authorities and external cyber security firms. Additional [illegible] will be published here.

LCX

Update January 9th, 2022

At roughly 11:23 PM CET on January 9th, LCX's Technology team detected unauthorized access of one crypto wallet at the LCX platform. A total of approx. 7.94M USD of crypto assets were stolen. 0.70M USD have been frozen. All other LCX wallets are not impacted.

During this difficult period we greatly appreciate the support from our customers, other exchanges, security experts, and the broader crypto community. LCX will continue to do everything in its power to mitigate the impact from this incident and restore full service as soon as possible.

Incident Details

The hacker wallet address is 0x165402279f2c081c54b00f0e08812f3fd4560a05.

The theft took place yesterday evening, January 8th 2022 between 11:23 PM and 11:37 PM CET.

During this period, the following cryptocurrencies were stolen:

Cryptocurrency (approx. USD value according to Coingecko):

- 162.68 ETH (502,671 USD)
- 3,437,783.23 USDC (3,437,783 USD)
- 761,236.94 EURe (864,840 USD)
- 101,249.71 SAND Token (485,995 USD)

An analysis of the hacker's address shows that consistent with the details publicly reported by LCX, between 01/08/2022 22:23 UTC and 22:35 UTC, various ERC-20 tokens were transferred from a wallet associated with LCX.

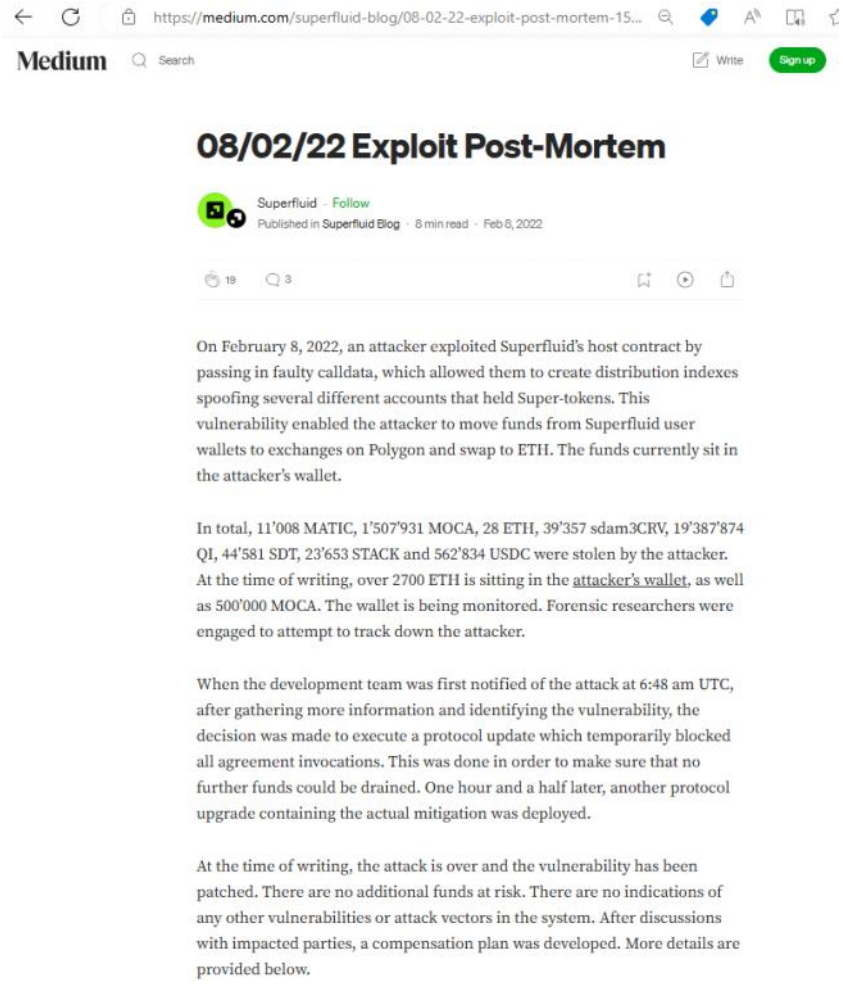
Also, on 01/08/2022 between 22:26 UTC and 22:37 UTC, about 162 ETH valued at approximately .43 million was transferred from an address associated with LCX to the hacker's wallet.

The ERC-20 tokens were then swapped between 01/08/2022 22:40 UTC and 01/10/2022 20:29 UTC for ETH.

Superfluid

Tuesday, September 24, 2024 2:28 PM

On 02/08/2022, Superfluid published a blog post on their official account on Medium.com titled "08/02/22 Exploit Post-Mortem". This post stated that on 02/08/2022 an attacker exploited Superfluid's protocol and was able to steal cryptocurrency.



In the blog post, the hacker's Polygon address was identified as 0x1574F7F4C9d3aCa2EbcE918e5d19d18aE853c090.

An analysis of this address shows that consistent with the post-mortem, the address received various tokens on 02/08/2022 6:17 UTC.

Hundred Finance

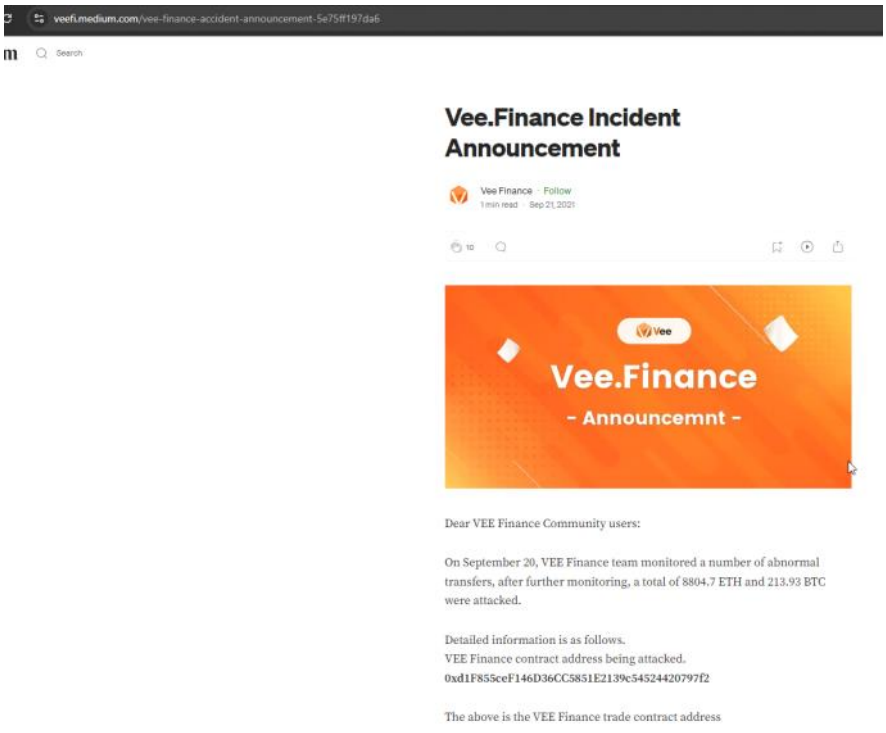
Tuesday, September 24, 2024 3:26 PM

On 03/15/2022, Hundred Finance confirmed on their official Twitter account that they had been hacked:

Vee Finance

Tuesday, September 24, 2024 3:36 PM

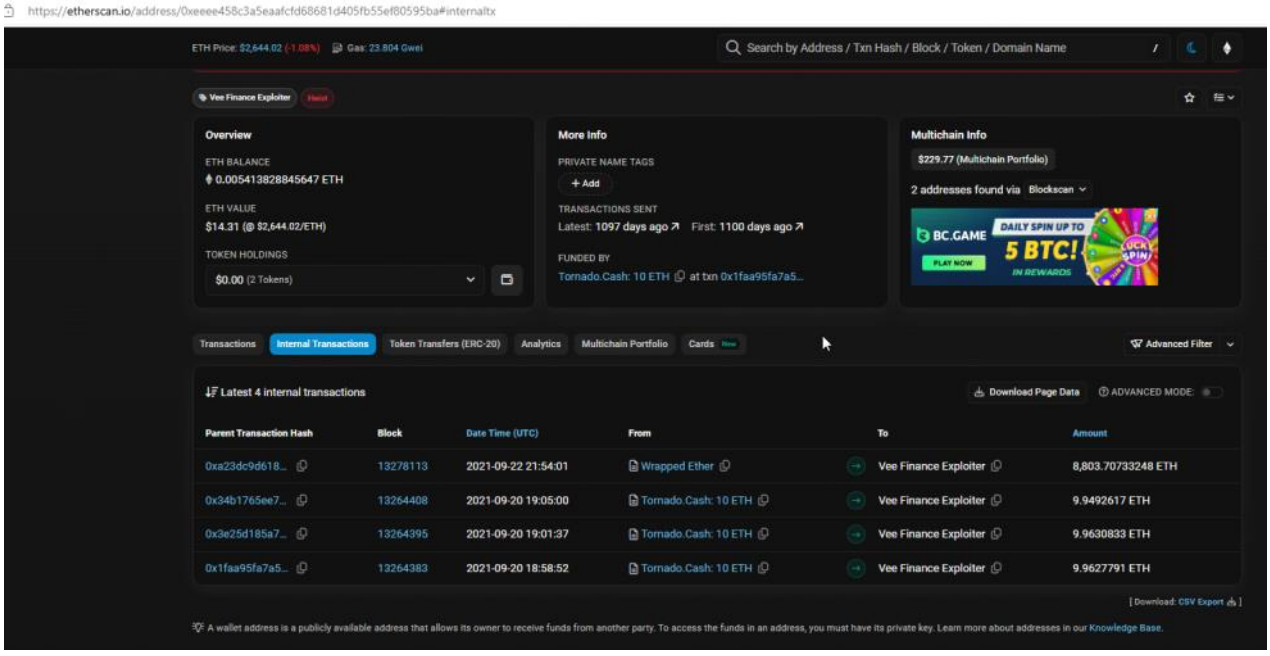
On 09/21/2021, Vee Finance announced via a blog post on their official Medium.com account that they had been hacked on 09/20/2021.



In this post they detail that various cryptocurrencies had been stolen and transferred into the attacker's address: 0xeeeE458C3a5eaAfcFd68681D405FB55Ef80595BA

Analyzing this address show that consistent with the blog post, between 09/20/2021 20:49 UTC and 09/21/2021 07:03 UTC, this address received a large amount of Wrapped BTC and Wrapped ETH.

On 09/22/2021 21:54 UTC, the hacker converted the Wrapped ETH to Ether, netting approximately 8,804 ETH valued at about $23.28 milli
on.



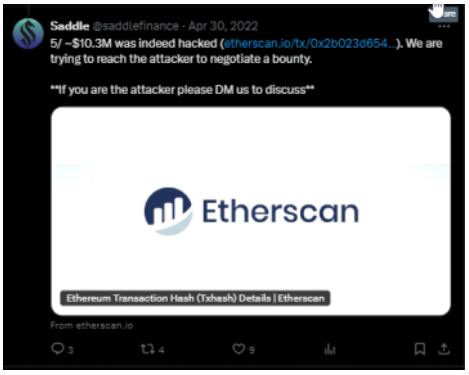
Between 09/22/2021 22:06 UTC and 09/22/2021 23:13 UTC, the hacker sent about 8,806 ETH to address 0xEe33902b81eb4b4A6988EB4Ebbf7E9A72fd2E0B6.

Saddle Finance

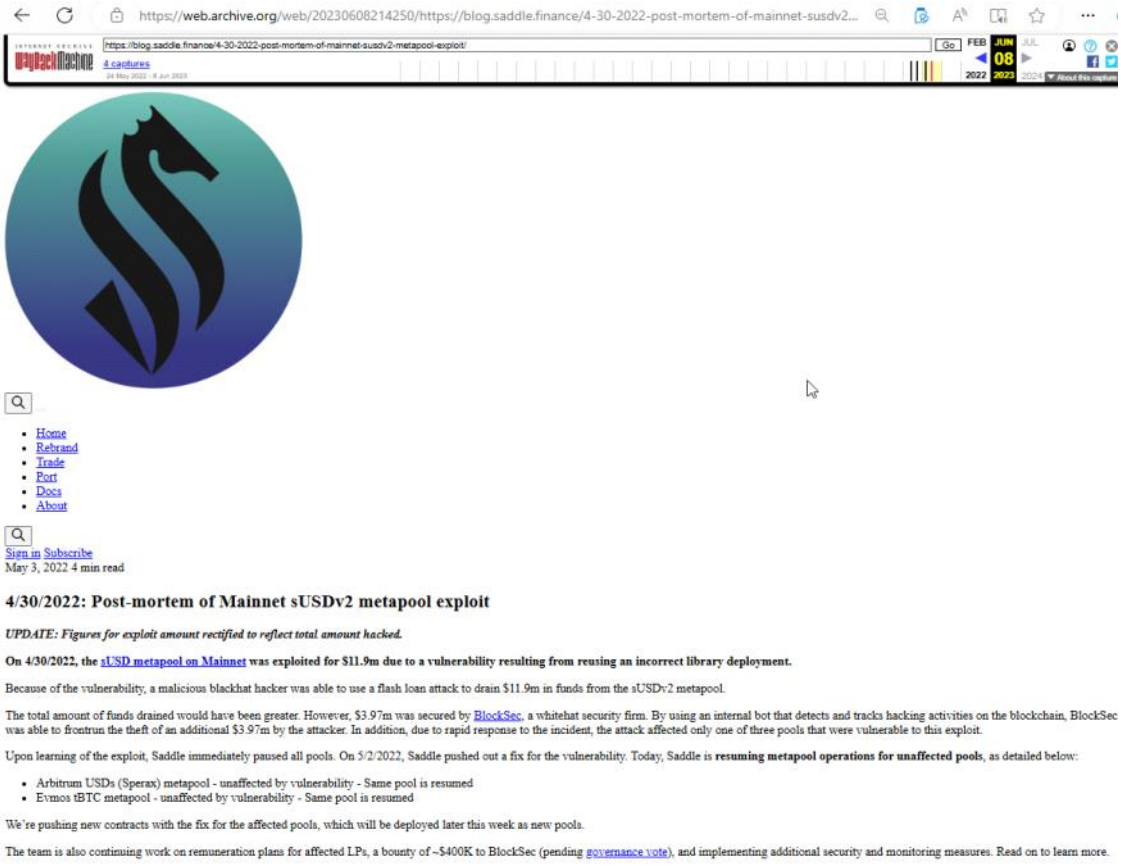
Tuesday, September 24, 2024 5:03 PM

On 04/30/2022, Saddle Finance announced via Twitter that their protocol had been hacked:

In another Twitter post, Saddle Finance states that $10.3 was hacked and they shared the Ethereum transaction associated with the hack:
0x2b023d65485c4bb68d781960c2196588d03b871dc9eb1c054f596b7ca6f7da56



On 05/03/2022, Saddle Finance published a now deleted blog on their website titled "Post-mortem of Mainnet sUSDv2 metapool exploit":



https://web.archive.org/web/20230608214250/https://blog.saddle.finance/4-30-2022-post-mortem-of-mainnet-susdv2...

https://blog.saddle.finance/4-30-2022-post-mortem-of-mainnet-susdv2-metapool-exploit/

4 captures

- Home
- Rebrand
- Trade
- Port
- Docs
- About

Sign in Subscribe
May 3, 2022 4 min read

4/30/2022: Post-mortem of Mainnet sUSDv2 metapool exploit

UPDATE: Figures for exploit amount rectified to reflect total amount hacked.

On 4/30/2022, the sUSD metapool on Mainnet was exploited for $11.9m due to a vulnerability resulting from reusing an incorrect library deployment.

Because of the vulnerability, a malicious blackhat hacker was able to use a flash loan attack to drain $11.9m in funds from the sUSDv2 metapool.

The total amount of funds drained would have been greater. However, $3.97m was secured by BlockSec, a whitehat security firm. By using an internal bot that detects and tracks hacking activities on the blockchain, BlockSec was able to frontrun the theft of an additional $3.97m by the attacker. In addition, due to rapid response to the incident, the attack affected only one of three pools that were vulnerable to this exploit.

Upon learning of the exploit, Saddle immediately paused all pools. On 5/2/2022, Saddle pushed out a fix for the vulnerability. Today, Saddle is **resuming metapool operations for unaffected pools**, as detailed below:

- Arbitrum USDs (Sperax) metapool - unaffected by vulnerability - Same pool is resumed
- Evmos tBTC metapool - unaffected by vulnerability - Same pool is resumed

We're pushing new contracts with the fix for the affected pools, which will be deployed later this week as new pools.

The team is also continuing work on remuneration plans for affected LPs, a bounty of ~$400K to BlockSec (pending governance vote), and implementing additional security and monitoring measures. Read on to learn more.

The post-mortem identifies two malicious transactions that drained the protocol of approximately $11.9 million in cryptocurrency.

The two malicious transactions were identified as:

https://etherscan.io/tx/0x2b023d65485c4bb68d781960c2196588d03b871dc9eb1c054f596b7ca6f7da56

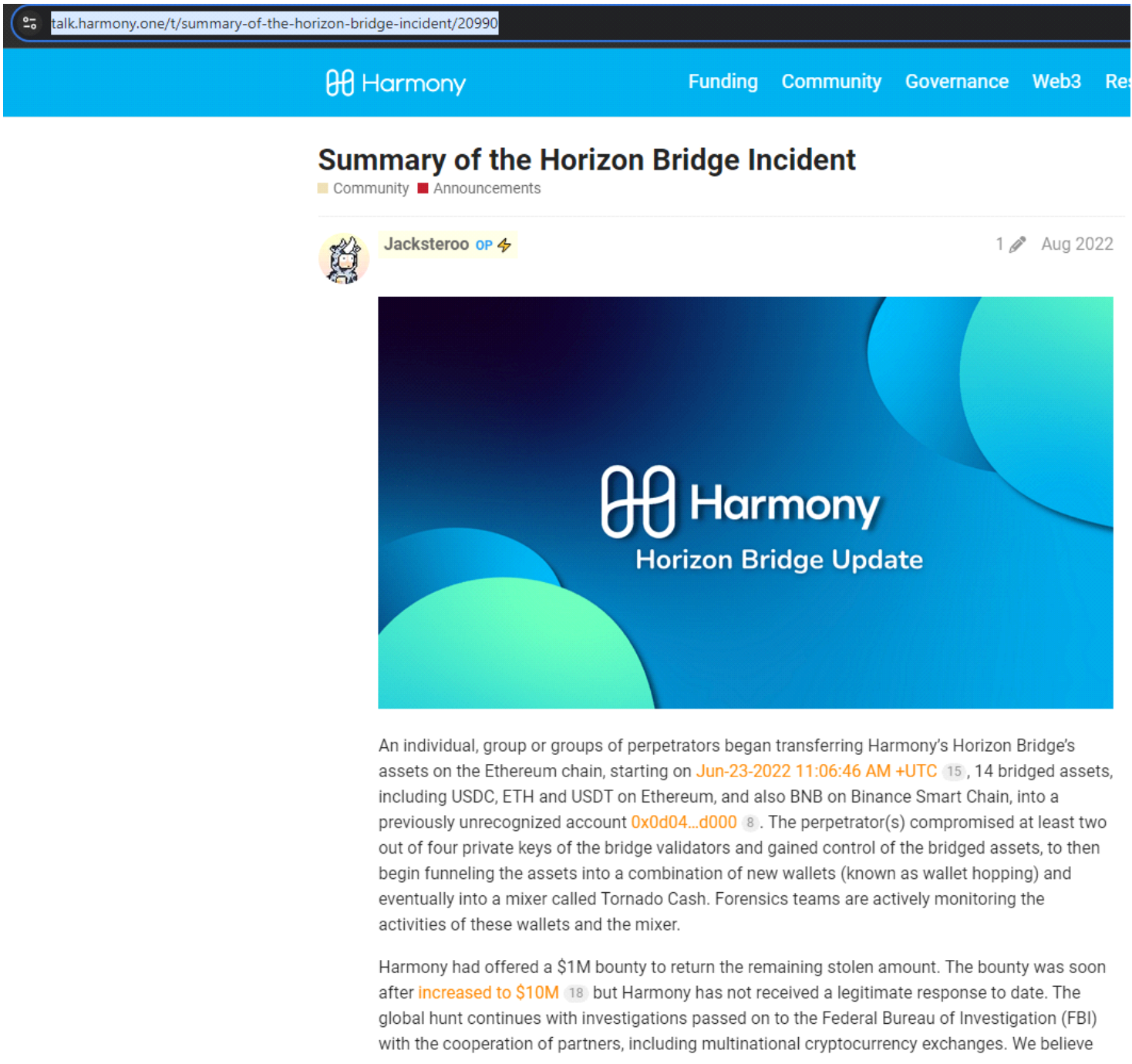
https://etherscan.io/tx/0xe7e0474793aad11875c131ebd7582c8b73499dd3c5a473b59e6762d4e373d7b8

An analysis of these transactions show that they were both ordered by address 0x63341Ba917De90498F3903B199Df5699b4a55AC0.

Harmony Horizon Bridge

Tuesday, September 24, 2024 5:30 PM

On 08/01/2022, Harmony published an article on their official website titled "Summary of the Horizon Bridge Incident". In the article they detail that they suffered an exploit on 06/23/2022 resulting in the loss of cryptocurrency. The article also identifies the hacker's Ethereum account:0x0d043128146654C7683Fbf30ac98D7B2285DeD00



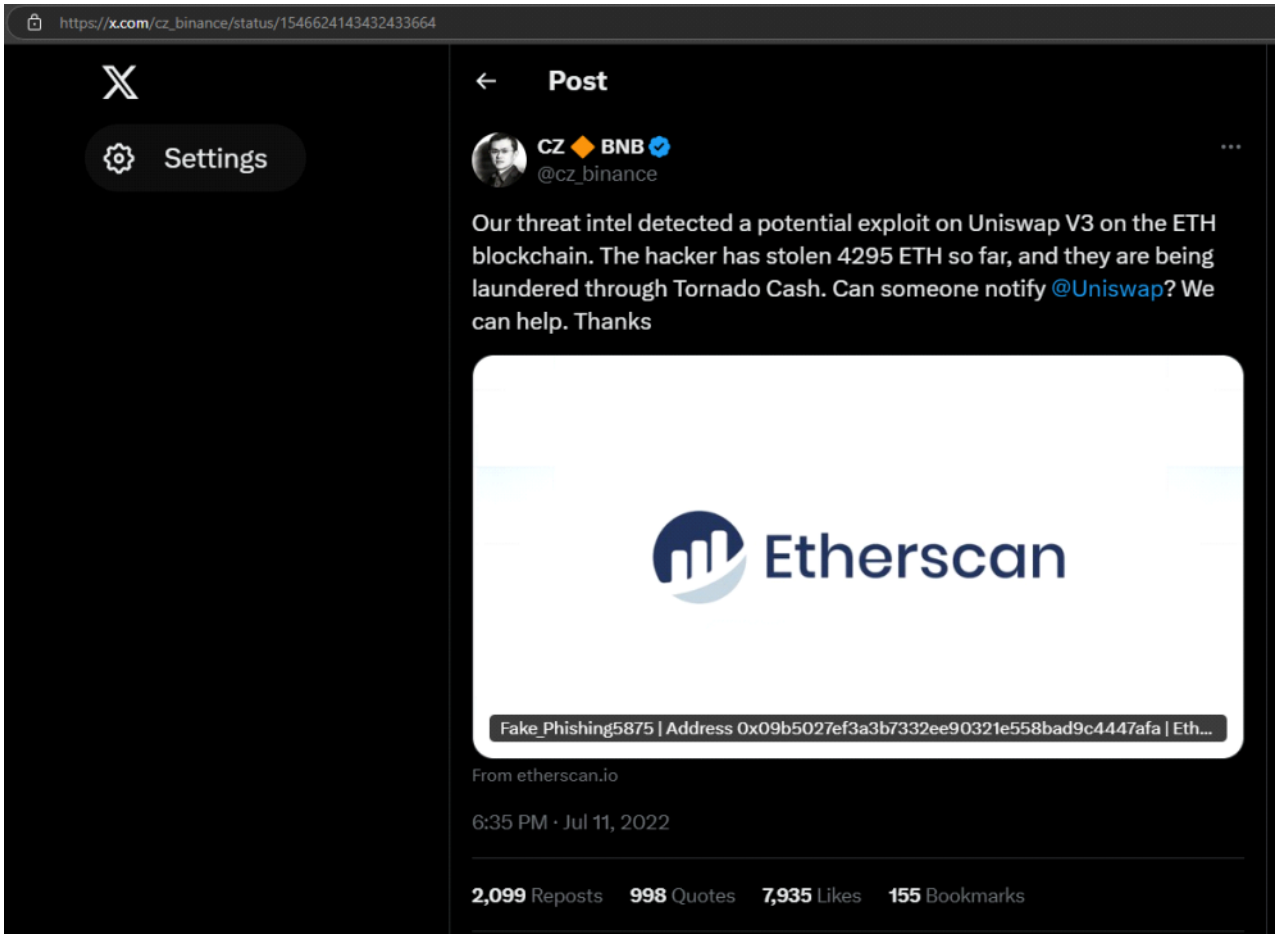
An analysis of the hacker's address shows that consistent with the incident summary, between 06/23/2022 11:08 UTC and 06/23/2022 11:26 UTC a large amount of ERC20 tokens were transferred from the Harmony Bridge. These tokens were swapped for Ether.

Between 06/27/2022 07:10 UTC and 07/01/2022 15:45 UTC, wallet 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 transferred 85,866 ETH to five intermediary

Uniswap Phishing

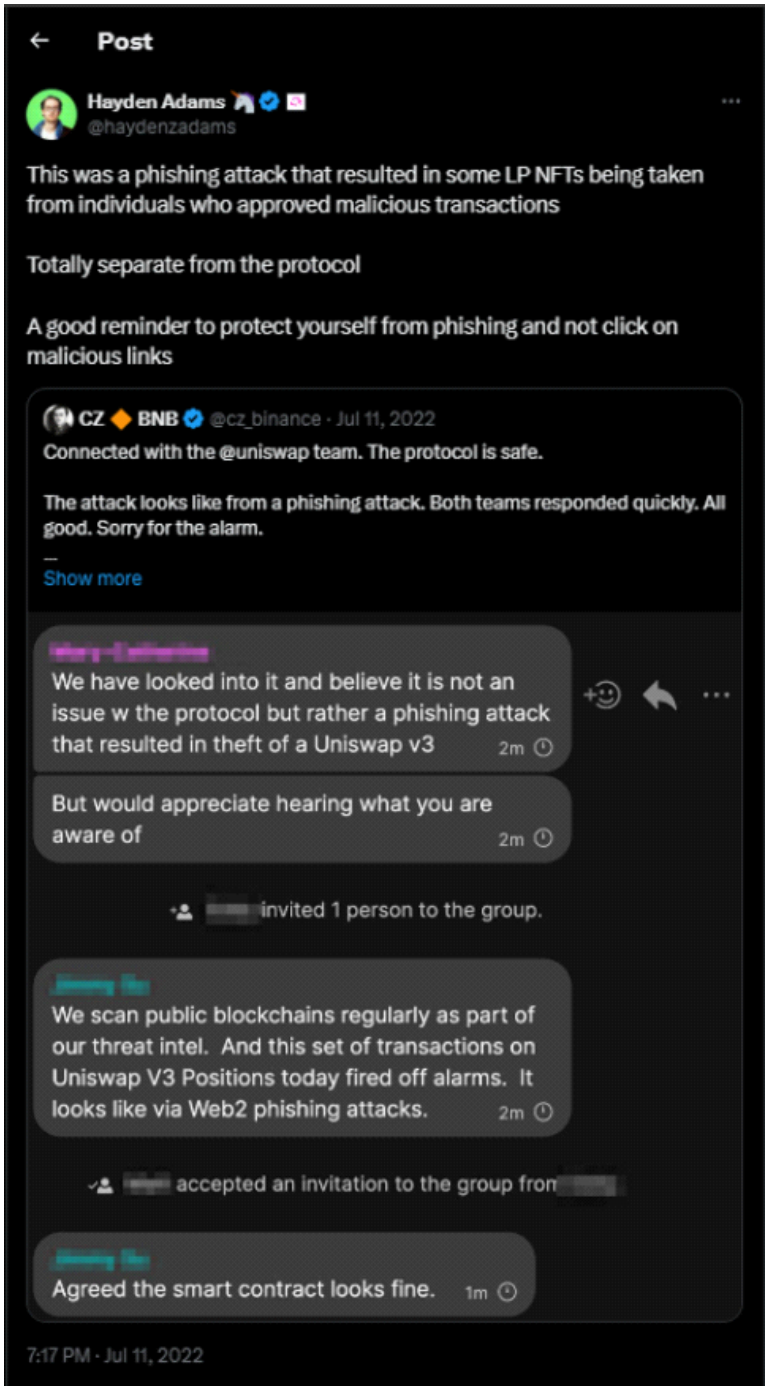
Saturday, October 19, 2024 7:42 PM

On July 11, 2022, the CEO of Binance Changpeng Zhao tweeted that there was a potential exploit with Uniswap and that Ether was being transferred to wallet 0x09b5027eF3a3b7332EE90321E558baD9C4447AFA:



The next day this was corroborated in a Tweet from Uniswap Labs:

Hayden Adams, the creator of Uniswap responded to CZ's tweets on the subject stating:

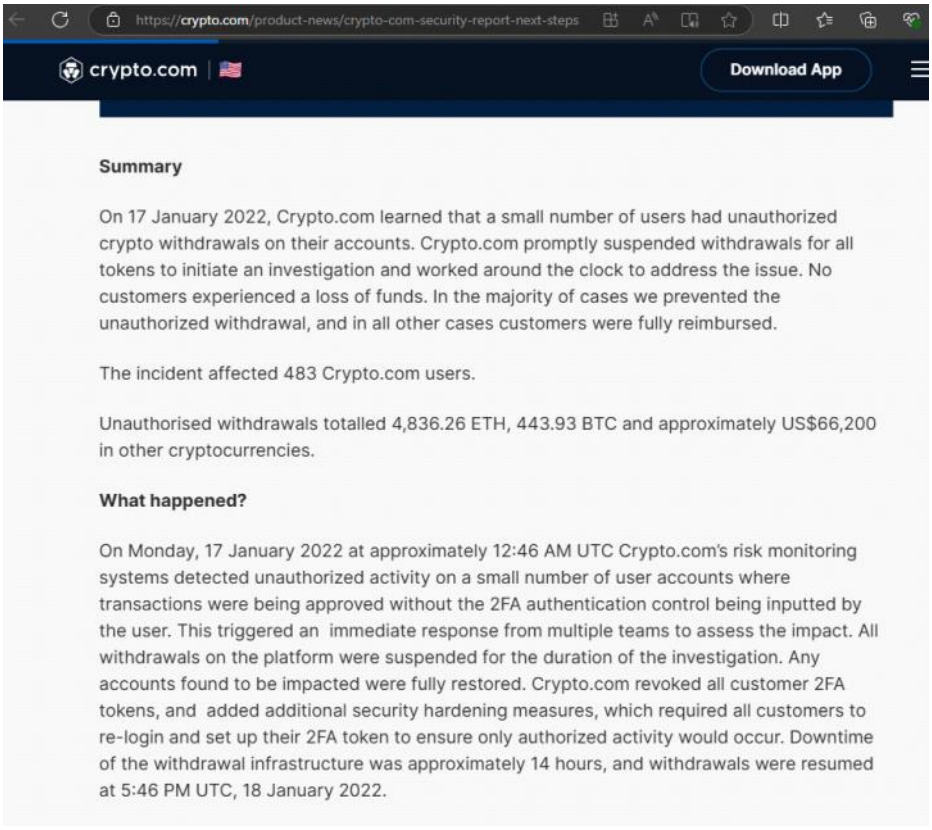


An analysis of Ethereum address 0x09b5027eF3a3b7332EE90321E558baD9C4447AFA shows that indeed it received about 240.41 Wrapped BTC on 07/11/2022 from an Ethereum address associated with Uniswap.

Crypto.com

Saturday, October 19, 2024 8:29 PM

On 01/20/2022 bitcoin exchange Crypto.com announced on their website that they had been hacked on 01/17/2022.



https://crypto.com/product-news/crypto-com-security-report-next-steps

crypto.com | 🇺🇸 Download App

Summary

On 17 January 2022, Crypto.com learned that a small number of users had unauthorized crypto withdrawals on their accounts. Crypto.com promptly suspended withdrawals for all tokens to initiate an investigation and worked around the clock to address the issue. No customers experienced a loss of funds. In the majority of cases we prevented the unauthorized withdrawal, and in all other cases customers were fully reimbursed.

The incident affected 483 Crypto.com users.

Unauthorised withdrawals totalled 4,836.26 ETH, 443.93 BTC and approximately US$66,200 in other cryptocurrencies.

What happened?

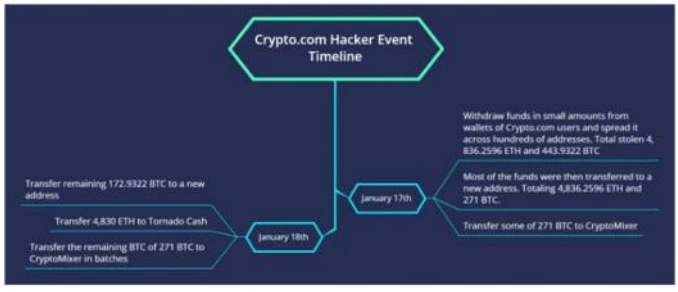
On Monday, 17 January 2022 at approximately 12:46 AM UTC Crypto.com's risk monitoring systems detected unauthorized activity on a small number of user accounts where transactions were being approved without the 2FA authentication control being inputted by the user. This triggered an immediate response from multiple teams to assess the impact. All withdrawals on the platform were suspended for the duration of the investigation. Any accounts found to be impacted were fully restored. Crypto.com revoked all customer 2FA tokens, and added additional security hardening measures, which required all customers to re-login and set up their 2FA token to ensure only authorized activity would occur. Downtime of the withdrawal infrastructure was approximately 14 hours, and withdrawals were resumed at 5:46 PM UTC, 18 January 2022.

On 08/19/2022, blockchain forensics firm SlowMist released their 2022 Mid-Year Report on Blockchain Incidents and Methods of Laundering. In their report, they identify the Crypto.com hacker's Ethereum address as 0x6e1218c55f1aCb588Fc5E55B721f1183D7D29D3d:

https://medium.com/coinmonks/2022-mid-year-report-on-blockchain-i...

- Crypto.com

Hackers Addresses:
0x6e1218c55f1aCb588Fc5E55B721f1183D7D29D3d (ETH)
bc1qk8wlwypvvr6v5lmsngg5a248k2a9cgrsrw5jsq (BTC)
bc1q83c9e7s8925hhy9dzqpdyyfctgwaspj3wdrhqr (BTC)
bc1qk7e2k8s252789cggr5xy67m6jvc0jsqpdjfw9d (BTC)
bc1qnzn9wmt40qwuhd7zmqvmvd0c3zazv59ljplrnr (BTC)
bc1qy7hf94vv20jqez2fk8xyxuv0h0u8r0kh8cau46 (BTC)
Date: 01/17/2022, 01/18/2022
Amount: 4,836.2596 ETH, 443.9322 BTC
InitialFunding: N/A
Event:



(Crypto.com Hacker — Timeline of Fund Transfers)